UTSA Libraries
1 0000 00377969 9

AMERICAN MATHEMATICAL SOCIETY COLLOQUIUM PUBLICATIONS

Volume VII

FRANK

C04322631

APR 27 1944

WITHDRAWN
UTSA LIBRARIES

QA
145
.B444
1927

D660691

LIBRARY
The University of Texas
at San Antonio

RENEWALS 458-4574

DATE DUE

DEC 13

GAYLORD

PRINTED IN U.S.A

AMERICAN MATHEMATICAL SOCIETY
COLLOQUIUM PUBLICATIONS, VOLUME VII

ALGEBRAIC ARITHMETIC

BY

ERIC T. BELL

PROFESSOR OF MATHEMATICS
CALIFORNIA INSTITUTE OF TECHNOLOGY

NEW YORK
PUBLISHED BY THE
AMERICAN MATHEMATICAL SOCIETY
501 WEST 116TH STREET
1927

LÜTCKE & WULFF, HAMBURG, GERMANY

LIBRARY
The University of Texas
At San Antonio

CONTENTS

PAGE

INTRODUCTION 1

CHAPTER I

VARIETIES OF ALGEBRA USEFUL IN ALGEBRAIC ARITHMETIC

1– 3. Irregular fields, modules, rays, rings, semigroups 5
4– 7. Characteristics of algebraic arithmetic 9
8– 9. One-rowed matrices 15
10–12. Matric fields 17
13–18. The associated functional varieties of $\mathfrak{U}_m$ 20
19–23. The irregular fields $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ associated with $\mathfrak{A}$. 27
24–26. The partitions of a matrix 30

CHAPTER II

THE ALGEBRA $\mathfrak{P}$ OF PARITY

1– 6. Absolute and relative parity 34
7– 9. Abstract identity of $\mathfrak{P}$ with the algebra $\mathfrak{T}$ of the circular functions 43
10–14. Expansion and decomposition in $\mathfrak{P}$ 47
15–17. The identical transformations in $\mathfrak{P}$ 51
18–21. Divisibility in $\mathfrak{P}$ 54
22. Algebraic parity, generalization of $\mathfrak{P}$ 63

CHAPTER III

THE ALGEBRAIC ARITHMETIC OF MULTIPLY PERIODIC FUNCTIONS

1– 6. The principle of paraphrase 64
6.1–11. Extension of the principle to higher forms 80
12–16. Application of the principle to theta quotients . 88
17–20. Application to theta functions of $p > 1$ arguments 106

CHAPTER IV

APPLICATIONS OF THE ALGEBRAS $\mathfrak{C}$, $\mathfrak{D}$

PAGE

1– 9. Algebra $\mathfrak{E}$ 112
10–12. The variety $\mathfrak{E}_r$ of $\mathfrak{E}$ 124
13–14. Extensions and further instances of $\mathfrak{E}$ 144
15–17. Applications of $\mathfrak{C}$ to the algebra of sequences . 146

CHAPTER V

ARITHMETICAL STRUCTURE

1– 2. Nature of general arithmetic 160
3– 7. Arithmetic $\mathfrak{L}_N$ of $\mathfrak{L}$ 165
8– 9. Arithmetization 175

INDEX 177

ALGEBRAIC ARITHMETIC

INTRODUCTION

1. Intermediate between the modern analytic theory of numbers and classic arithmetic as developed by the school of Gauss, is an extensive region of the theory of numbers where the methods of algebra and analysis are freely used to yield relations between integers expressed wholly in finite terms and without reference, in the final propositions, to the operations or concepts of limiting processes. This part of the theory of numbers we shall call *algebraic arithmetic*. Its boundaries are not sharply defined, nor is it desirable that they should be, as power comes from flexibility and almost any part of arithmetic can be profitably employed in any other. Nevertheless there is a large, growing and somewhat uncoordinated body of results, with many aims and methods peculiar to itself, which falls into neither the classic theory of numbers nor the modern developments of the analytic and algebraic theories, and this region, which we have called algebraic arithmetic, offers many suggestive opportunities for systematic exploration. It is the purpose of the following chapters to outline a few promising directions in which progress may be made toward classifying, extending and generalizing the methods and results of algebraic arithmetic. The insistence will be upon general methods rather than specific applications, as the latter are so numerous, and so readily made from the general formulations, that it will be sufficient merely to indicate occasionally a few of them to lend concreteness to the abstract theories. What is given here is but a narrow cross section of a very extensive field.

2. The distinction between analytic and algebraic arithmetic is evident from the comparison of two famous theorems. Let $F(n)$ = the number of representations of n as a sum of 4 integer squares, $s(n)$ = the sum of all the odd divisors of n; $\pi(x)$ = the number of primes $\leq x$. Then

$$F(n) = 8[2+(-1)^n]\,s(n), \qquad \lim_{x\to\infty} \pi(x)/(x/\log x) = 1.$$

The first accords with the general description in § 1; the second belongs to a totally different order of ideas. They have in common one feature however which is of more than merely historical interest: both were discovered by transcendental methods. The first has since been proved in many ways in the manner traditionally called elementary in arithmetic; from its nature the second is incapable of such proof.

The numerous proofs which have been devised for the 4-square theorem, or for its less complete form which asserts that every integer is the sum of 4 squares, certainly one of the perfect gems of arithmetic, emphasize the advantages in the theory of numbers of multiplying proofs for the light which such revaluations of known theorems throw upon the theories in which they originate. This particular theorem has enriched, and has been enriched by the theories of elliptic functions, quaternions and their generalizations, and Dickson arithmetics. Starting from Jacobi's elementary recasting of the transcendental proof by means of elliptic functions, for instance, Liouville states that, following Dirichlet, he was led to the discovery of his powerful general formulas in the theory of numbers which he published without proofs, and thence back, by a natural reaction, to an interesting generalization of elliptic functions — which has not yet been fully explored. Again, Euler's early attempts to prove that every integer is the sum of 4 squares gave him his identity which, in modern phrase, is the theorem for the norm of the product of two quaternions; this in turn suggested to Graves, Roberts, Cayley and others purely algebraic investigations which have again reacted on the theory of numbers through Dickson's arithmetics.

3. From our point of view in the present theory it is little to the purpose to offer as an objection against a transcendental proof the remark that a purely elementary demonstration is in existence or may be found. A transcendental proof often exhibits the advantages inherent in the impulses to generalization and unification characteristic of analysis. But it must not be forgotten, on the contrary, that a finite, strictly elementary proof as frequently fertilizes an otherwise barren waste of algebra by the introduction of new arithmetical concepts or processes. Neither the transcendental nor the elementary method can be fruitfully used for long to the exclusion of the other. If occasionally we seem to go out of our way to make the elementary transcendental our apology is that analytical proofs, judged by the ease with which they are retained and applied, are altogether more elementary than many in the theory of numbers which depend upon nothing more advanced than the rudiments of algebra. The principal reason however for our emphasis of transcendental methods is their power, suggestiveness, and the readiness with which they yield themselves to generalization. Incidentally it may be remarked that even the most elementary proofs in the theory of numbers are tainted by the transcendence inherent in mathematical induction and in the notion of "any integer n".

4. In the description of algebraic arithmetic we have used several terms whose significance is usually taken by consent as being obvious, but which will be clearly understood only when large tracts of extant arithmetic have been subjected to the postulational method. Among these is arithmetic itself. It is generally conceded that an arithmetic, as distinguished from an algebra, must be based on integral elements. There exists however no set of postulates sufficiently elastic to embrace all the known instances of elements called integral by their creators. An abstract logical analysis, culminating in the relational formulation of existing arithmetical theories should disclose the essential characteristics common to all. In the absence of even partial analysis of this kind for the

fundamental concepts of arithmetic we shall offer tentatively a definition to justify our subsequent characterization of certain theories as arithmetical, and to this we turn first. The algebraic varieties (rings, irregular fields, matric fields, etc.,) encountered in this attempt are valuable instruments in algebraic arithmetic, independently of whether they may ultimately yield a satisfactory description of arithmetic itself. We shall therefore state their postulate systems in full.

For easy reference the several varieties indicated by German capitals have been included in the index at the end of the book.

CHAPTER I

VARIETIES OF ALGEBRA USEFUL IN ALGEBRAIC ARITHMETIC

IRREGULAR FIELDS, MODULES, RAYS, RINGS, SEMIGROUPS, §§ 1-3

1. Common algebra, abstract identity. By *common algebra* $\mathfrak{A}$ we shall mean the set of all propositions, including Π, implied by the set Π of postulates of the abstract field $\mathfrak{F}$ in which the notations are as usual: $a+b$, ab denote the sum, product of any two elements a, b in $\mathfrak{F}$; the zero, unity in $\mathfrak{F}$ are written 0, 1, and Π is as in Dickson, *Algebras and their Arithmetics* (1st edition, p. 200). This Π is identical with that stated in § 2 if there we take $m = 1$. The fields of all complex, rational numbers are denoted by $\mathfrak{F}_c$, $\mathfrak{F}_r$ respectively.

The elements and operations of $\mathfrak{A}$ are abstract in the sense of marks without significance beyond that implied by the assertion of Π. By assigning to the elements and operations of $\mathfrak{A}$ specific interpretations I_j $(j = 1, 2, \cdots)$ such that the resulting systems $\mathfrak{A}_j$ are consistent with Π (and with I_j), we obtain *instances* $\mathfrak{A}_j$ of $\mathfrak{A}$, and $\mathfrak{A}_j$, $\mathfrak{A}_k$ are said to be *identical* or *distinct* according as I_j, I_k are the same or different; $\mathfrak{A}$ and distinct $\mathfrak{A}_j$ $(j = 1, 2, \cdots)$ are said to be *abstractly identical*. The simplest $\mathfrak{A}_j$ are $\mathfrak{F}_c$, $\mathfrak{F}_r$.

A system obtained from $\mathfrak{A}$ by modification (including suppression) of one or more of the postulates Π will be called a *variety*. In any variety $\mathfrak{V}$ definitions precisely similar to those for $\mathfrak{A}$ concerning instances and abstract identity are presupposed. Varieties will be designated by German capitals.

2. Irregular fields. $\mathfrak{U}$ consists of a set Σ of elements $\alpha, \beta, \cdots, \gamma, \cdots$ and two operations S, P (called *addition, multiplication*) which may be performed upon any two distinct or identical elements α, β of Σ, in this order, to produce

uniquely determined elements $S\{\alpha, \beta\}$, $P\{\alpha, \beta\}$ in Σ (this is a postulate), such that the postulates (2.1)-(2.5) are satisfied. Elements of Σ will be called *elements* of $\mathfrak{U}$, and similarly in all like cases.

(2.1) If α, β are any two elements of $\mathfrak{U}$, then

$$S\{\beta, \alpha\} = S\{\alpha, \beta\}, \quad P\{\beta, \alpha\} = P\{\alpha, \beta\}.$$

(2.2) If α, β, γ are any three elements of $\mathfrak{U}$, then

$$S\{S\{\alpha,\beta\},\gamma\} = S\{\alpha, S\{\beta,\gamma\}\}, \quad P\{P\{\alpha,\beta\},\gamma\} = P\{\alpha, P\{\beta,\gamma\}\},$$
$$P\{\alpha, S\{\beta, \gamma\}\} = S\{P\{\alpha, \beta\}, P\{\alpha, \gamma\}\}.$$

(2.3) There exist in $\mathfrak{U}$ two distinct elements, denoted by ζ, v, such that, if α is any element of $\mathfrak{U}$,

$$S\{\alpha, \zeta\} = \alpha, \quad P\{\alpha, v\} = \alpha.$$

(2.4) Whatever be the element α of $\mathfrak{U}$ there exists in $\mathfrak{U}$ an element α' such that $S\{\alpha, \alpha'\} = \zeta$.

(2.5) Whatever be the element β of $\mathfrak{U}$ different from each of the m ($\geqq 1$) distinct elements ζ_j ($j = 0, \cdots, m-1$), where $\zeta_0 \equiv \zeta$, of $\mathfrak{U}$, there exists in $\mathfrak{U}$ an element β' such that $P\{\beta, \beta'\} = v$.

The ζ_j ($j = 0, \cdots, m-1$) in (2.5) are called *irregular*, all other elements of $\mathfrak{U}$ *regular*; $S\{\alpha, \beta\}$, $P\{\alpha, \beta\}$ in (2.1) are called the *sum*, *product* of α, β, and ζ, v in (2.3) the zero, unity of $\mathfrak{U}$. An instance of $\mathfrak{U}$ is said to be *regular* or *irregular* according as $m = 1$ or $m > 1$; when $\mathfrak{U}$ contains precisely m irregular elements we indicate this by writing $\mathfrak{U}_m$, and instances of $\mathfrak{U}$ are designated by accents, thus $\mathfrak{U}'_m, \mathfrak{U}''_m, \cdots$. Hence $\mathfrak{U}'_1 = \mathfrak{A} = \mathfrak{F}$. We shall write $\mathfrak{U}_\infty = \mathfrak{J}\mathfrak{F}$, and call $\mathfrak{J}\mathfrak{F}$ an *irregular field*.

By slight modifications of Dickson's proofs for $\mathfrak{F}$ we have the following basic theorems for $\mathfrak{U}_m$ and hence for $\mathfrak{J}\mathfrak{F}$.

(2.6) ζ, v are unique in $\mathfrak{U}_m$.

(2.7) $S\{\alpha, \beta\} = S\{\alpha, \gamma\}$ implies $\beta = \gamma$. Hence α in (2.4) is unique; it is called the *negative* of α.

(2.8) If α, β are in $\mathfrak{U}_m$ there exists in $\mathfrak{U}_m$ a unique ξ such that $S\{\alpha, \xi\} = \beta$.

(2.9) If α, β, γ are in $\mathfrak{U}_m$ and $P\{\alpha, \beta\} = P\{\alpha, \gamma\}$, and if α is regular, then $\beta = \gamma$. Hence β' in (2.5) is unique.

(2.10) If α, β are in $\mathfrak{U}_m$ and α is regular, there exists in $\mathfrak{U}_m$ a unique θ such that $P\{\alpha, \theta\} = \beta$; θ is called the *quotient of β by α*; if $\beta = v$, θ is called the *reciprocal* of α. It is sufficient, and frequently shorter, to replace division by α by multiplication by the reciprocal of α. To show that division in a given variety is possible in the sense of (2.10) it suffices to prove that a regular element has a unique reciprocal. This remark will be found useful in some of the more complicated instances occurring later.

The consistency of the postulates is proved as we proceed by exhibiting numerous instances of varieties which satisfy them.

For the following remarks on $\mathfrak{U}_m$, which place $\mathfrak{U}_m$ with respect to linear algebra, I am indebted to Professor Wedderburn. Let Ψ be a cummutative linear associative algebra, of which the algebra $\Omega = (\zeta_0, \zeta_1, \cdots, \zeta_{m-1})$, with $\zeta_0 = \zeta$, is an invariant subalgebra. Then $\mathfrak{U}_m$ is the difference algebra $\Psi - \Omega$, and equality in $\mathfrak{U}_m$ can be interpreted as "congruent mod Ω", also v is the identity element of Ψ. If Ω is maximal and Ψ commutative, $\mathfrak{U}_m = \Psi - \Omega$ is necessarily a field.

The varieties $\mathfrak{F}$, $\mathfrak{J}\mathfrak{F}$ and several of their instances $\mathfrak{F}'$, $\mathfrak{J}\mathfrak{F}'$, $\cdots$ are fundamental for algebraic arithmetic, as also are the following.

3. Modules, rays, rings, commutative semigroups. Denote for the moment by S, P, P_{-1}, S_{-1} addition, multiplication, division and subtraction in $\mathfrak{U}_m$, P_{-1}, S_{-1} being given by (2.10), (2.7), and write $(O\,T\cdots)$ for a variety closed under operations 0, T, $\cdots$, together with those operations. Then in $\mathfrak{U}_m$ we have 15 conceivable subvarieties $(S^a P^b P_{-1}^c S_{-1}^d)$, where each of a, b, c, $d = 0$ or 1. We shall require only the following in addition to $\mathfrak{U}_m$: the *module*, $\mathfrak{M} \equiv (S_{-1})$, $= (SS_{-1})$; the *ray*, (PP_{-1}); the *ring*, $\mathfrak{R} = (SPS_{-1})$. Thus in $\mathfrak{A}$ we have the varieties commonly designated by the same names;

a module of $\mathfrak{A}$ is a set in $\mathfrak{A}$ closed under addition and subtraction in $\mathfrak{A}$; a ray of $\mathfrak{A}$ is an abelian group in $\mathfrak{A}$ under multiplication in $\mathfrak{A}$; a ring of $\mathfrak{A}$ is a system in $\mathfrak{A}$ closed under addition, multiplication and subtraction in $\mathfrak{A}$. These cases are of particular importance later.

Instead of the ray we shall generally use the commutative semigroup, which differs from the ray in that reciprocals do not necessarily exist in the system, although cancellation of common factors from equal products is legitimate. For brevity we confine the following to the case corresponding to $\mathfrak{A}$; the postulates are practically those of Dickson (*Transactions*, vol. 6, 1905, pp. 205–208).

A *semigroup* $\mathfrak{G}$ is a system consisting of a set Σ_G of elements $\alpha, \beta, \cdots, \gamma, \cdots$ and an operation P which may be performed upon any two distinct or identical elements α, β of Σ_G, in this order, to produce a uniquely determined element $P_G(\alpha, \beta)$ of Σ_G such that the postulates (3.1)–(3.3) are satisfied. P is called *multiplication*, $P_G(\alpha, \beta)$ the *product* of α, β; elements of Σ_G are called *elements* of $\mathfrak{G}$.

(3.1) If α, β, γ are any elements of $\mathfrak{G}$ then

$$P_G(P_G(\alpha, \beta), \gamma) = P_G(\alpha, P_G(\beta, \gamma)).$$

(3.2) If α, β, γ are elements of $\mathfrak{G}$ such that $P_G(\alpha, \beta) = P_G(\alpha, \gamma)$, then $\beta = \gamma$.

(3.3) If α, β, γ are elements of $\mathfrak{G}$ such that $P_G(\beta, \alpha) = P_G(\gamma, \alpha)$, then $\beta = \gamma$.

It is shown by Dickson that any left unity μ of multiplication, $P_G(\mu, \alpha) = \alpha$ for each α in $\mathfrak{G}$, is also a right unity, $P_G(\alpha, \mu) = \alpha$, and further that the existence of μ implies that not more than one *reciprocal* α' exists for each α in $\mathfrak{G}$, viz., $P_G(\alpha, \alpha') = \mu$ for α in $\mathfrak{G}$ has one solution α' or none.

Adjoining to (3.1)–(3.3) two further postulates,

(3.4) $P_G(\alpha, \beta) = P_G(\beta, \alpha)$,

(3.5) There exists in $\mathfrak{G}$ a *unity* μ; $P_G(\alpha, \mu) = P_G(\mu, \alpha) = \alpha$,

we shall call the $\mathfrak{G}$ satisfying (3.1)–(3.5) a *commutative semigroup* with *unity* μ.

CHARACTERISTICS OF ALGEBRAIC ARITHMETIC, §§ 4–7

4. Instances of arithmetical theories. According to the fundamental theorem of rational arithmetic a positive integer is uniquely the product of positive primes; a prime is the product of no two integers both different from units. Similar definitions hold in the theory of algebraic numbers where, however, the fundamental theorem fails and where also it is necessary to distinguish between primes in a ring and elements of the ring indecomposable with respect to multiplication. It will be sufficient here merely to recall a few of the principal definitions in order to lend reasonableness to our subsequent description of algebraic arithmetic.

If α, β are any elements of a ring $\mathfrak{R}$ of algebraic numbers, and if the G. C. D.* of α, β exists and is in $\mathfrak{R}$, then $\mathfrak{R}$ is said (by J. König, *Algebraische Größen*, Leipzig, 1903) to be a complete holoid domain. Let $\mathfrak{R}$ be such. Elements of $\mathfrak{R}$ differing only by unit† factors are called *equivalent*. An *indecomposable* element γ of $\mathfrak{R}$ has no factor in $\mathfrak{R}$ not equivalent to γ or to the absolute unit 1; if π is in $\mathfrak{R}$ and is such that π divides a product $\alpha\beta$ of two elements α, β in $\mathfrak{R}$ only when π divides at least one of α, β, π is called prime in $\mathfrak{R}$. An indecomposable element in $\mathfrak{R}$ is not in general prime in $\mathfrak{R}$. The fundamental theorem (unique factorization into primes) holds for finite products in $\mathfrak{R}$.

An algebraic integer is a root of an algebraic equation with rational integer coefficients, that of the highest power of the unknown being unity. The rational integers are therefore algebraic, but the failure in general of the fundamental theorem shows that the generalization implied in this remark

* The G. C. D. is defined thus, and an abstractly identical definition is assumed in any variety where the G. C. D. is significant: If δ divides α and β, and if δ contains every γ which divides α and β, then δ is called the G. C. D. of α and β. Likewise for the L. C. M.: If μ is a multiple of α and β, and if μ is contained in every ϱ which is a multiple of α and β, then μ is called the L. C. M. of α and β.

† A *unit* in $\mathfrak{R}$ is an element of $\mathfrak{R}$ which divides every element of $\mathfrak{R}$, the quotient being also in $\mathfrak{R}$. Similarly, when significant, for units in any variety.

is but partial; the strictly arithmetical character of the theory is attained only by passing to elements (ideals in Dedekind's theory, ideal numbers in the theories of Zolotareff, Prüfer, v. Neumann and others) beyond the original data (algebraic integers). In this respect the multiplicative theory of algebraic integers is abstractly identical with no part of classical rational arithmetic, for in the latter the fundamental theorem subsists for the original integral elements themselves. If however the rational integers be replaced by the principal ideals which they define (in rational arithmetic), abstract identity, for multiplicative arithmetic only, is achieved.

The above remarks are intended merely to suggest the difficulties inherent in an attempt to state inclusively the essential distinction between an algebraic theory and one that may properly, in accordance with accepted instances. be called arithmetical. As it is one of the major projects of algebraic arithmetic to discover abstract identities between rational arithmetic and arithmetic in given instances of varieties, we shall attempt next to frame a definition of arithmetic which shall preserve the characteristic features of the classical theories just described and be applicable to several extensive tracts of the theory of the rational and algebraic numbers. The following may be regarded as a tentative first approximation to a postulation of arithmetic. Note that all postulates in what precedes (and the like applies to subsequent varieties) have been so framed as to exclude divisors of irregular elements, and in particular divisors of zero.

5. Restricted and complete arithmetical theories. Let $\mathfrak{G}$ be a commutative semigroup with unity μ. If μ has divisors in $\mathfrak{G}$ ($\equiv$ elements of $\mathfrak{G}$ whose product is μ), they will be called *units*; μ in any case is included in the units. Elements of $\mathfrak{G}$ differing only by unit factors are *equivalent*; in what follows equivalent elements are regarded as identical. Then, if and only if there exists in $\mathfrak{G}$ a subset Σ of elements which is such that no element of Σ is the product of two elements of Σ both different from units, and each element

of $\mathfrak{G}$ except μ that is not in Σ is the product of elements of Σ in one way only (apart from permutations of the factors), and further $\mathfrak{G}$ contains at least one element other than μ, we shall call $\mathfrak{G}$ an *arithmetical semigroup*. We say that $\mathfrak{G}$ is *proper* or *improper* according as the number of factors in the unique multiplicative decomposition of elements of Σ is or is not finite for each element of Σ. In any instance $\mathfrak{G}_j$ of $\mathfrak{G}$ we write Σ_j for Σ, and μ_j for μ. It need not be discussed here whether improper $\mathfrak{G}$'s exist.

Let $\mathfrak{A}_j$ be an instance of $\mathfrak{A}$. Then, if and only if it be possible to segregate from all the elements of $\mathfrak{A}_j$ a ring $\mathfrak{R}_j$ from whose elements can be constructed a set $\mathfrak{S}_j$ of functions forming an arithmetical semigroup $\mathfrak{G}_j$, shall we say that $\mathfrak{A}_j$ has (with respect to $\mathfrak{G}_j$) a *restricted arithmetical theory*; if in addition the elements of $\mathfrak{G}_j$ form a ring, we shall say that $\mathfrak{A}_j$ has with respect to $\mathfrak{G}_j$ a *complete arithmetical theory*. And in each case the theory is *proper* or *improper* with $\mathfrak{G}_j$. "Arithmetical theory", unless otherwise stated shall mean proper (restricted or complete) arithmetical theory.

Similarly, if in the above $\mathfrak{A}_j$, $\mathfrak{A}$ be replaced by any instance $\mathfrak{V}_j$ of any variety $\mathfrak{V}$ for which the concepts of ring and semigroup are significant, including the case $\mathfrak{V} = \mathfrak{R}$, $\mathfrak{V}_j = \mathfrak{R}_j$, we define the two species of arithmetical theories for these varieties.

In these definitions *function* is to be understood in its widest sense: if x, y are elements of any kind such that y is known when x is assigned, y is called a function of x. For example, to illustrate an instance much used presently, if the x_j are any elements of $\mathfrak{V}$, and x is the matrix $(x_1, x_2, \cdots, x_n)$, then the matrix $y = (x_a, x_b, \cdots, x_c)$, where $a, b, \cdots, c$ are definite integers chosen from the set $1, 2, \cdots, n$, is a function of x.

Write for a moment a_j, m_j, s_j for addition, multiplication and subtraction in $\mathfrak{R}_j = (a_j\ m_j\ s_j)$, and d_j for division in $\mathfrak{A}_j$. Then $\mathfrak{A}_j = (a_j\ m_j\ d_j\ s_j)$, while multiplication m_j' in $\mathfrak{G}_j$ is in general distinct from m_j.

To illustrate the last remark, in rational arithmetic we have m_j, m_j' identical, $\mathfrak{R}_j$ being here the ring of all rational

integers and Σ_j the set of all rational primes; $\mathfrak{S}_j = \mathfrak{R}_j$, $\mu_j = 1$. In the theory of algebraic numbers $\mathfrak{R}_j$ is the ring of all algebraic integers in a given algebraic number field $\mathfrak{A}_j$, while the elements (= functions) in $\mathfrak{S}_j$ are the ideals constructed from elements of $\mathfrak{R}_j$; m_j is now multiplication of algebraic integers, m_j' in $\mathfrak{S}_j$ is multiplication of ideals, and Σ_j is the set of prime ideals, μ_j = the unit ideal. Hence, in the sense defined above, Dedekind's theory is restricted; rational arithmetic and the revised theories of algebraic numbers due to Prüfer (*Mathematische Annalen*, vol. 94, 1925–6) and v. Neumann are instances of complete arithmetical theories. Our definitions are therefore not vacuous.

6. Additive and multiplicative arithmetic. Complete arithmetical theories are rare, as arithmetic has developed historically into two comparatively immiscible parts, the additive and the multiplicative. This separation extends to algebraic arithmetic. In additive arithmetic we are concerned with those properties of numbers which cluster about addition, in multiplicative with those springing from multiplication, primality, and the unique factorization law.

For additive arithmetic, in $\mathfrak{F}_c$, $\mathfrak{F}_r$ the appropriate analytical machinery is the theory of power series of a single variable, for multiplicative the theory of Dirichlet series of one dimension—the common species. Each of these is susceptible of an n-fold generalization, giving the corresponding theories for sets of $n \geqq 1$ integers. It will be sufficient to develop the theory for $n = 1$, as the theory for $n > 1$ can be placed in (1,1) correspondence with that for $n = 1$ by a well known device due to Gauss and used by Kronecker and others in the theory of algebraic numbers to pass from polynomials in 1 indeterminate to the like for several. The associated algebraic varieties are the module and the ring for additive, and the ray or the semigroup, preferably the latter, for multiplicative arithmetic. These also have n-fold generalizations, based on the like for $\mathfrak{U}_m$, but we shall attend only to the case $n = 1$.

In the analytical theory of numbers convergence and limiting processes are central; in algebraic arithmetic infinite processes

in the usual sense enter only incidentally and can always be replaced by elementary algorithms. Hence we shall replace the entire algebra of power series in $\mathfrak{F}_c, \mathfrak{F}_r$ by a variety $\mathfrak{C}$, a special $\mathfrak{JF}$, whose elements are matrices (one-rowed in the case discussed here) of infinite order, and similarly for $\mathfrak{D}$ and Dirichlet multiplication. Both $\mathfrak{C}$ and $\mathfrak{D}$ are very special instances of what we shall call a matric field, which also includes many further varieties useful in algebraic arithmetic, and this itself is an instance of $\mathfrak{JF}$. By this means we put transcendental algebraic arithmetic on a sound abstract basis. When infinite processes are used in the sequel as in ordinary analysis, convergence of course is essential, and if it is only occasionally mentioned where relevant, for example in the theta and elliptic expansions, this is because all the processes occurring are either known to be convergent or may be shown to be so by simple means. From $\mathfrak{C}, \mathfrak{D}$ will be constructed in a subsequent chapter a more recondite variety $\mathfrak{E}$, the algebra of primality and unique factorization, which yields for any $\mathfrak{JF}$ and for any instance of $\mathfrak{A}$ a complete arithmetical theory of considerable interest. Both $\mathfrak{C}$ and $\mathfrak{D}$ illustrate Wedderburn's theory of algebras lacking a finite basis (*Transactions*, vol. 26, 1924, pp. 395–426); $\mathfrak{E}$ is apparently of a different species.

7. Crosses and possible generalizations. Attempts to cross fertilize the additive and multiplicative sections of arithmetic invariably lead to serious difficulties. Thus the classic theory of partitions is additive; one of its earliest hybrids is the arithmetic theory of forms, including Waring's theorem; another is Goldbach's conjecture. Again, no satisfactory definition (unless it may be in the recent attempts of Prüfer and v. Neumann) has been evolved for the addition of ideals.

There is however one striking exception in this discouraging prospect. The theory of the multiply periodic functions provides an inexhaustible store of additive-multiplicative properties of the rational integers. Nor is this limited, as in the classical developments of this branch of arithmetic, to diophantine

equations and inequalities of the second degree. An extensive class of interesting problems of any degree may be investigated by the general arithmetical formulas furnished by the theta functions of $p \geqq 1$ variables and their quotients. For this a variety $\mathfrak{P}$, discussed in detail in the next chapter, emerges as fundamental. In the elaboration of $\mathfrak{P}$ several instances of the varieties already defined appear as useful accessories. For all of $\mathfrak{C}$, $\mathfrak{D}$, $\mathfrak{E}$, $\mathfrak{P}$ and a fifth instance $\mathfrak{B}$ of $\mathfrak{FF}$, useful in the study of sequences of numbers or functions, certain preliminaries concerning one-rowed matrices (or vectors) are indispensable.

Before proceeding to these we may point out three ways in which the concept of an arithmetical theory admits of generalization. The first we have already mentioned: all that follows can be recast with n-fold ($n > 1$) series and products as a background; this leads to the n-fold generalizations of the varities used here, and can be placed in (1.1) correspondence with them. Next, if we regard unicity of decomposition, the evident aspect of atomicity, as it were, as the essence of arithmetic, we are not confined to multiplication and its consequent $\mathfrak{G}$ in the definitions of indecomposable and primes, but may base an arithmetic on addition, or on any of the operations indicated presently.

At least one instance of an arithmetical theory founded on primality with respect to addition exists, namely in Prüfer's theory of ideal numbers (not ideals in the usual sense), which possess a unique additive decomposition.

Finally there is the possible extension of all that precedes to n-adic relations, $n > 2$, of which a specific example is the multiplicative theory of matrices in space of n dimensions. In any of the foregoing instances there are the further opportunities of developing the arithmetic (as defined here) of the varieties obtained by modifying the postulate systems of any given varieties, e. g., by suppressing the commutative law. As a clue to an implicit arithmetic any quality of uniqueness is worth following and elaborating. This yields for example, the germ of an arithmetic of geometry, in which

uniqueness resides in the determination of one class by two or more classes. We return to this in the final chapter.

ONE-ROWED MATRICES, §§ 8-9

8. C, D matrices, scalars, products, functions in $\mathfrak{V}$. For subsequent use we need a few simple concepts concerning one-rowed matrices. As most of these are not current they demand detailed definition. The following is continued in § 24.

A set is a collection of elements without reference to arrangement; if the collection be arranged according to any law it becomes a one-rowed matrix, in which any given order of the elements may be taken as normal. Two normal types will be considered: the C, in which the suffixes of the elements run $0, 1, \cdots$, and the D, in which they run $1, 2, \cdots$. Thus $(z_0, z_1, \cdots, z_n)$ is a *C matrix of order $n+1$*, $(z_1, z_2, \cdots, z_n)$ a *D matrix of order n*. The C, D types refer respectively to additive and multiplicative arithmetic; when it is unnecessary to draw a distinction either the C or the D may be used. If all the elements of a matrix are in a given variety $\mathfrak{V}$, the matrix is said to be *in* $\mathfrak{V}$. If $z_a, z_b, \cdots, z_c$ is any subset of the elements of any matrix, the normal order is that in which the suffixes are in ascending order. Thus if $a < b < \cdots < c$, the normal matrix constructed from $z_a, z_b, \cdots, z_c$ is $(z_a, z_b, \cdots, z_c)$. By a mere change in the notation of the elements any matrix can be written in either the C or the D form. In all applications the matrices may be replaced if desired by the sets in which they originate, but as this yields no essential gain in generality, and as it is always shorter to use the derived matrices, we shall attend exclusively to the latter. The elements of our matrices $x, y, \cdots$ belong to a variety $\mathfrak{V}$ or they are themselves such matrices. In the latter case the matrix may be represented as a rectangular array of elements of $\mathfrak{V}$, but this, as will appear, is no advantage.

Equality of matrices, $z = w$, where $z \equiv (z_k, z_{k+1}, \cdots, z_n)$, $w \equiv (w_k, w_{k+1}, \cdots, w_n)$, and $k = 0$ or 1 according as both of z, w are C or D, is defined as usual: $z = w$ when and only when $z_j = w_j$ $(j = k+1, \cdots, n)$.

Elements of the $\mathfrak{V}$ in which the matrices $x, y, \cdots$ under consideration lie will be called *scalars*. The *order* of a matrix is the number of elements it contains; in any case the kind of element, scalar or matric, unless clear from the context must be stated. This applies particularly to $\mathfrak{P}$, in which $\mathfrak{V} \equiv \mathfrak{A}$. A scalar may be regarded as a matrix of unit order.

With z, w as above, and t scalar, the *product* tz of t and z is $(tz_k, tz_{k+1}, \cdots, tz_n)$. In particular, $-z = -1z = (-z_k, \cdots, -z_n)$. If $u, v, \cdots w, z$ are matrices, and $z \equiv (u, v, \cdots, w)$, than by definition $tz \equiv (tu, tv, \cdots, tw)$. If the elements of z, w are scalars, the *scalar product* of z and w is the scalar

$$(zw) \equiv z_k w_k + z_{k+1} w_{k+1} + \cdots + z_n w_n;$$

the *absolute product* $|zw|$ is the matrix

$$|zw| \equiv (z_k w_k, z_{k+1} w_{k+1}, \cdots, z_n w_n),$$

in both of which the indicated multiplications and additions, if significant, are those of the $\mathfrak{V}$ in which the matrices are defined; if $\mathfrak{V}$ has neither addition nor multiplication, (zw) does not exist; if multiplication is lacking, zw does not exist. The matric product of z, w, less useful for our purpose, is noticed later. The *zero matrix* $(\zeta)_n$ of order n in $\mathfrak{V}$ has each of its n elements = the zero, ζ, in $\mathfrak{V}$.

We shall presuppose the concept of functions in $\mathfrak{V}$. Briefly, if $x, y, \cdots, t$ are in a given class $\mathfrak{S}$ of sets, then φ is called *a uniform function* of $x, y, \cdots, t$ over $\mathfrak{S}$ in $\mathfrak{V}$, or simply a *function*, as we shall have no occasion to use non-uniform functions, and $\mathfrak{V}$, $\mathfrak{S}$ in each instance will be plain from the context. There is an extended significance of functions which also is useful. Let $\mathfrak{V}'$, $\mathfrak{V}''$ be distinct varieties, and let $\varphi(x', y', \cdots, z')$ be a function in $\mathfrak{V}'$ as just defined. By means of a correspondence between $\mathfrak{V}'$, $\mathfrak{V}''$ it may happen that when $\varphi(x', y', \cdots, z')$ is known there is a unique determination or value, of $\psi(x'', y'', \cdots, z'')$ in $\mathfrak{V}''$, and hence

$\psi(x'', y'', \cdots, z'')$ can be regarded as a function of x', $y', \cdots, z'$.

Variables, constants and parameters in $\mathfrak{V}$ are defined as usual in an obvious way.

9. Matric variables in $\mathfrak{V}$. A matrix in $\mathfrak{V}$ is a function. Thus, as a particular instance of an implicit function in $\mathfrak{V}$ we have $\varphi(u, v, \cdots, w)$, where $u, v, \cdots, w$ are matrices, a type which is fundamental in the algebraic arithmetic of multiply periodic functions. The following also is of special importance in the same connection and elsewhere, notably in $\mathfrak{P}$ and its generalizations.

The independent scalar variables $x, y, \cdots, z$ of any function can be separated into mutually exclusive sets which may then be normally ordered into matrices. By referring to a function of such matrices we do not restrict the generality of the function discussed; the same function can also be considered as a function of all the independent variables composing the matrices, and reference to the latter merely isolates certain aspects of the function which we wish to investigate. We shall frequently discuss functions from both points of view simultaneously, considering in different connections the matrices or the independent variables composing them as the "variables" of the functions. To distinguish these we shall call a matrix of scalar variables a *matric variable*, reserving the term *variable* to mean variable scalar. The *order* of a matric variable is the number of variables it contains; the definition of a *value* of a matric variable is implicit in what precedes. The following is basic for the algebra of functions of 2 matric variables, which in turn are important in additive and multiplicative arithmetic.

MATRIC FIELDS, §§ 10–12

10. Partial D addition and multiplication S_j, P_j. Return now to § 2 and let $a, b, \cdots, c, z, u, \cdots$ be the set Σ_D of all D matrices of order n in $\mathfrak{U}_m$, the notation being so chosen that the n elements of any element ($=$ matrix) in Σ_D are indicated by the Greek letter with suffixes $1, \cdots, n$

corresponding to the Latin letter which denotes the matrix, thus $a \equiv (\alpha_1, \cdots, \alpha_n)$, $b \equiv (\beta_1, \cdots, \beta_n), \cdots$, the $\alpha_j, \beta_j, \cdots$ $(j = 1, \cdots, n)$ being in $\mathfrak{U}_m$. Parentheses ( ) are used exclusively in §§ 10, 11 for elements of Σ_D, curled brackets { } for functions in $\mathfrak{U}_m$ of precisely two elements of Σ_D; the functions considered are $S_j\{a, b\}$, $P_j\{a, b\}$ $(j = 1, \cdots, n)$ where a, b are any two elements of Σ_D. Hence $S_j\{x, y\}$, $P_j\{x, y\}$ are significant if and only if x, y are in Σ_D and $1 \leqq j \leqq n$, while $(\eta_1, \cdots, \eta_n)$ is significant if and only if η_j $(j = 1, \cdots, n)$ are in $\mathfrak{U}_m$. It will be observed that these conditions are fulfilled in the postulates stated presently. *The elements* $u \equiv (u_1, \cdots, u_n)$, $z \equiv (z_1, \cdots, z_n)$ *of* Σ_D *are special,* and are defined by the postulate (10.3). Any element $d = (\delta_1, \cdots, \delta_n)$ of Σ_D whose first element δ_1 is irregular in $\mathfrak{U}_m$ is called *irregular* in Σ_D; all other elements of Σ_D are *regular*; u, z are called the *unity, zero* in Σ_D.

For $j = 1, 2, \cdots, n$ the postulates (10.1)–(10.5) for $S_j\{a, b\}$, $P_j\{a, b\}$ are to be satisfied, where a, b are any two equal or distinct elements of Σ_D.

(10.1) For each pair of elements a, b of Σ_D, in this order, $S_j\{a, b\}$, $P_j\{a, b\}$ are uniquely determined elements of $\mathfrak{U}_m$, and

$$S_j\{b, a\} = S_j\{a, b\}, \qquad P_j\{b, a\} = P_j\{a, b\}.$$

(10.2) If a, b, c are any three elements of Σ_D, then

$$S_j\big\{(S_1\{a, b\}, \cdots, S_n\{a, b\}), c\big\} = S_j\big\{a, (S_1\{b, c\}, \cdots, S_n\{b, c\})\big\},$$

$$P_j\big\{(P_1\{a, b\}, \cdots, P_n\{a, b\}), c\big\} = P_j\big\{a, (P_1\{b, c\}, \cdots, P_n\{b, c\})\big\},$$

$$P_j\big\{a, (S_1\{b, c\}, \cdots, S_n\{b, c\})\big\}$$
$$= S_j\big\{(P_1\{a, b\}, \cdots, P_n\{a, b\}), (P_1\{a, c\}, \cdots, P_n\{a, c\})\big\}.$$

(10.3) If and only if $a' = z$ is $S_j\{a, a'\} = \alpha_j$ for every element $a \equiv (\alpha_1, \cdots, \alpha_n)$ of Σ_D; if and only if $b' = u$ is $P_j\{b, b'\} = \beta_j$ for every element $b \equiv (\beta_1, \cdots, \beta_n)$ of Σ_D.

(10.4) Whatever be the element c of Σ_D there exists in Σ_D a unique element c'' such that $S_j\{c, c''\} = z_j$.

(10.5) Whatever be the regular element e of Σ_D there exists in Σ_D a unique element e''' such that $P_j\{e, e'''\} = u_j$.

That (10.1)–(10.5) are not vacuous will be proved when, as presently, we exhibit several instances. The system has indeed an infinity of solutions, of which at least three, to be discussed shortly, are fundamental for algebraic arithmetic.

The functions $S_j\{a, b\}$, $P_j\{a, b\}$ are called *the jth partial sum, product in Σ_D of a, b*; the unique c'' in (10.4) is called the *negative in Σ_D of c*, and e''' in (10.5) the *reciprocal in Σ_D of e*. The set Σ_D, closed under jth partial addition, multiplication ($j = 1, \cdots, n$) yields the following instances of $\mathfrak{U}_m$.

11. **The D matric field $\mathfrak{D}_n\,\mathfrak{U}_m$ of order n in $\mathfrak{U}_m$.** With the same notations as in § 10, write as definitions of S_D, P_D,

$$S_D\{a, b\} \equiv (S_1\{a, b\},\ S_2\{a, b\}, \cdots, S_n\{a, b\}),$$
$$P_D\{a, b\} \equiv (P_1\{a, b\},\ P_2\{a, b\}, \cdots, P_n\{a, b\}).$$

The set Σ_D of all D matrices of order n in $\mathfrak{U}_m$ is an instance of $\mathfrak{U}_m$, say $\mathfrak{D}_n\,\mathfrak{U}_m$, in which the sum of any two equal or distinct elements a, b of Σ_D is $S_D\{a, b\}$ and the product is $P_D\{a, b\}$. The irregular elements, the negative of any element c, the reciprocal of any element e and the zero, unity in $\mathfrak{D}_n\,\mathfrak{U}_m$ are identical respectively with the irregular elements, the negative of c, the reciprocal of e, and the zero, unity in Σ_D.

To prove this it is sufficient to observe that S_D, P_D are instances of S, P in § 2, when Σ in § 2 is replaced by Σ_D.

12. **The C matric field $\mathfrak{C}_n\,\mathfrak{U}_m$ of order n in $\mathfrak{U}_m$.** Return to § 10 and rewrite all D matrices as C matrices of order $n+1$, $n \geq 0$, viz., the suffixes now run $0, 1, 2, \cdots, n$, and change the range of j to $j = 0, 1, \cdots, n$. Then, for example, the first of the postulates in (10.2) becomes, ($j = 0, \cdots, n$),

$$S_j\big\{(S_0\{a, b\}, \cdots, S_n\{a, b\}), c\big\} = S_j\big\{a, (S_0\{b, c\}, \cdots, S_n\{b, c\})\big\}.$$

By such obvious changes we define jth partial sums, products in the set Σ_C of all C matrices in $\mathfrak{U}_m$. Replacing D throughout § 11 by C we obtain the abstractly identical C theorem which specifies $\mathfrak{C}_n\,\mathfrak{U}_m$.

Thus far the $\mathfrak{X}_n\,\mathfrak{U}_m$, $\mathfrak{X} \equiv \mathfrak{C}, \mathfrak{D}$, are the same instance of $\mathfrak{U}_m$ in different notations. The commutative semigroups $\mathfrak{G}_X$ introduced in § 16 differentiate the $\mathfrak{X}_n\,\mathfrak{U}_m$ into distinct species, additive and multiplicative with respect to arithmetic, and they verify what follows through instances of jth partial multiplication P_j in § 10.

THE ASSOCIATED FUNCTIONAL VARIETIES OF $\mathfrak{U}_m$, §§ 13—18

13. The X associated functions of a matrix. What immediately follows can be stated for either $\mathfrak{X}$ in $\mathfrak{X}_n\,\mathfrak{U}_m$ of §§ 11, 12. We shall give full definitions for $\mathfrak{X} \equiv \mathfrak{D}$ and thence, as in § 12, infer the abstractly identical set for $\mathfrak{X} \equiv \mathfrak{C}$. The notation is as in §§ 11, 12; addition, multiplication in the instances $\mathfrak{X}_n\,\mathfrak{U}_m$ of $\mathfrak{U}_m$ are indicated by S_X. P_X, while in $\mathfrak{U}_m$ they are S, P; the elements of $\mathfrak{X}_n\,\mathfrak{U}_m$ are $a, b, c, \cdots, t, u, z, \cdots$ in X notation, u, z, being the unity, zero. We operate simultaneously in $\mathfrak{U}_m$, $\mathfrak{X}_n\,\mathfrak{U}_m$.

Let $t \equiv (\tau_1, \tau_2, \cdots, \tau_n)$ be the element of $\mathfrak{D}_n\,\mathfrak{U}_m$ whose first element $\tau_1 = v$ (the unity in $\mathfrak{U}_m$), and whose remaining $n-1$ elements τ_j $(j = 2, \cdots, n)$ are parameters in $\mathfrak{U}_m$, and let $a \equiv (\alpha_1, \cdots, \alpha_n)$ be any element $\neq t$ of $\mathfrak{D}_n\,\mathfrak{U}_m$. Then the scalar product $\varphi_D\{a, t\}$ in $\mathfrak{U}_m$ of a, t,

$$\varphi_D\{a, t\} \equiv S\big\{P\{\alpha_1, \tau_1\}, P\{\alpha_2, \tau_2\}, \cdots, P\{\alpha_n, \tau_n\}\big\}$$

is called the D *associated function* (in $\mathfrak{U}_m$) of the element a (of $\mathfrak{D}_n\,\mathfrak{U}_m$) with the *parameter* t.

Making the indicated changes from D to C notation we define $\varphi_C\{a, t\}$. If n is finite an instance of $\varphi_X\{a, t\}$ in F_c is a polynomial in an nth root of unity; if n is infinite an instance in F_c is an infinite series in one complex variable; other instances in a Galois field (n finite) are evident.

The following developments are of extreme generality; they provide a basis for the construction of an unlimited number

of theories arithmetical in the sense already described. Their important significance for infinite processes in $\mathfrak{A}$, and hence in its instances $\mathfrak{F}_j$ $(j = c, r)$ will be pointed out in § 15.

14. The functional varieties $\mathfrak{X}_{n,\varphi}\,\mathfrak{U}_m$ $(\mathfrak{X} = \mathfrak{C}, \mathfrak{D})$. *The set $\Sigma_{X,\varphi}$ of all X associated functions $\varphi_X\{w, t\}$ of the elements w of $\mathfrak{X}_n\,\mathfrak{U}_m$ having the parameter t is an instance $\mathfrak{X}_{n,\varphi}\,\mathfrak{U}_m$ of $\mathfrak{U}_m$ under the postulates* (14.1)–(14.5), *in which addition, multiplication are indicated by $S_{X,\varphi}$, $P_{X,\varphi}$.*

(14.1) The elements of $\mathfrak{X}_{n,\varphi}\,\mathfrak{U}_m$ are identical with those of $\Sigma_{X,\varphi}$.

(14.2) Two elements $\varphi_X\{a, t\}$, $\varphi_X\{b, t\}$ are equal in $\mathfrak{X}_{n,\varphi}\,\mathfrak{U}_m$, $\varphi_X\{a, t\} = \varphi_X\{b, t\}$, when and only when $a = b$ in $\mathfrak{X}_n\,\mathfrak{U}_m$, and hence also when and only when coefficients of like parameters τ_j are equal.

(14.3) The zero, unity in $\mathfrak{X}_{n,\varphi}\,\mathfrak{U}_m$ are $\varphi_X\{z, t\}$, $\varphi_X\{u, t\}$, where z, u are the zero, unity in $\mathfrak{X}_n\,\mathfrak{U}_m$.

(14.4) The irregular elements of $\mathfrak{X}_{n,\varphi}\,\mathfrak{U}_m$ are the $\varphi_X\{j, t\}$, where j runs through all irregular elements of $\mathfrak{X}_n\,\mathfrak{U}_m$.

(14.5) The sum, product, difference of any two elements $\varphi_X\{a, t\}$, $\varphi_X\{b, t\}$ of $\mathfrak{X}_{n,\varphi}\,\mathfrak{U}_m$, and the quotient of $\varphi_X\{a, t\}$ by any regular element $\varphi_X\{c, t\}$, are identical respectively with the elements $\varphi_X\{s, t\}$, $\varphi_X\{p, t\}$, $\varphi_X\{d, t\}$, and $\varphi_X\{q, t\}$, where s, p, d are respectively the sum, product, difference in $\mathfrak{X}_n\,\mathfrak{U}_m$ of a, b, and q is the quotient in $\mathfrak{X}_n\,\mathfrak{U}_m$ of a by b.

From the last therefore,

$$S_{X,\varphi}\big\{\varphi_X\{a, t\},\ \varphi_X\{b, t\}\big\} = \varphi_X\big\{S_X\{a, b\}, t\big\},$$
$$P_{X,\varphi}\big\{\varphi_X\{a, t\},\ \varphi_X\{b, t\}\big\} = \varphi_X\big\{P_X\{a, b\}, t\big\};$$

the quotient $\varphi_X\{q, t\}$ is defined by

$$P_{X,\varphi}\big\{\varphi_X\{q, t\},\ \varphi_X\{c, t\}\big\} = \varphi_X\{a, t\}, \qquad P_X\{q, c\} = a,$$

and similarly for the difference on replacing P by S and suppressing the restriction that $\varphi_X\{c, t\}$ be regular. That $\mathfrak{X}_{n,\varphi}\,\mathfrak{U}_m$ is indeed an instance of $\mathfrak{U}_m$ is evident.

15. Triple isomorphism of $\mathfrak{U}_m$, $\mathfrak{X}_n\,\mathfrak{U}_m$, $\mathfrak{X}_{n,\varphi}\,\mathfrak{U}_m$. *If*

(15) $$I\{\mathfrak{a}, \mathfrak{b}, \cdots, \mathfrak{c}\} = \mathfrak{z}$$

is an identity in any one of the varieties $\mathfrak{U}_m$, $\mathfrak{X}_n\mathfrak{U}_m$, $\mathfrak{X}_{n,q}\mathfrak{U}_m$, *3 denoting the zero in that variety, it is also an identity in each of the others.* It is implied in this statement that irregular elements do not occur as divisors.

This is obvious, since each variety is an instance of $\mathfrak{U}_m$. Moreover *if* (15) *be an identity in* $\mathfrak{U}_m$, *its instance in* $\mathfrak{X}_n\mathfrak{U}_m$ *can be inferred from that in* $\mathfrak{X}_{n,q}\mathfrak{U}_m$ *by equating coefficients of like parameters* τ_j *in the latter, and applying to the result the definition of equality of matrices.*

The effect of the last is to replace operations upon X matrices by abstractly identical operations in $\mathfrak{X}_{n,q}\mathfrak{U}_m$ upon their respective X associated functions. Since $\mathfrak{A}$ is an instance of $\mathfrak{U}_m$, and $\mathfrak{F}_j(j = c, r)$ are instances of $\mathfrak{A}$, the theorems apply in particular to $\mathfrak{F}_j(j = c, r)$. When $n = \infty$ the instances in $\mathfrak{F}_j(j = c, r)$ of the theorem are equivalent to the statement of the necessary and sufficient conditions that those operations upon infinite series commonly called formal (but preferably algebraic) shall be legitimate and hence lead to correct conclusions. When the elements of the instance of $\mathfrak{U}_m$ concerned are neither real nor complex numbers the theorem (when $n = \infty$) defines the use of infinite series which have no numerical significance and for which convergence is therefore without meaning. The numerous algorithms to which this theorem leads are powerful instruments of unification and generalization in algebraic arithmetic.

16. **The associated semigroup $\mathfrak{G}_X$ of $\mathfrak{X}_n\mathfrak{U}_m$.** Let $a \equiv (\alpha_1, \cdots, \alpha_n)$, $b \equiv (\beta_1, \cdots, \beta_n)$ be any elements of $\mathfrak{D}_n\mathfrak{U}_m$, and $t \equiv (\tau_1, \cdots, \tau_n)$ the parameter of any element $\varphi_D\{a, t\}$ of $\mathfrak{D}_{n,\varphi}\mathfrak{U}_m$, so that $\tau_1 =$ the unity v in $\mathfrak{U}_m$, in which addition, multiplication are indicated by S, P as always. To simplify the printing put for a moment $m_k \equiv \mu$, $\tau(j) \equiv \tau_j$, $\alpha(j) \equiv \alpha_j$, $\beta(j) \equiv \beta_j$ $(j = 1, \cdots, n)$.

Suppose now that the $\tau_j(j = 1, \cdots, n)$ form with respect to P a semigroup $\mathfrak{G}_D$. Then $\mathfrak{G}_D$ has the unity $\tau(1)$ and is commutative. Let all pairs $(\tau(i), \tau(j))$ of solutions in $\mathfrak{G}_D$ of

$$P\{\tau(i), \tau(j)\} = \tau(k),$$

for k constant, $1 \leqq k \leqq n$, be given by

$$(i, j) \equiv (i_s, j_s) \qquad (s = 1, \cdots, \mu),$$

and write as the definition of $p_k\{a, b\}$,

$$p_k\{a, b\} \equiv S\Big\{P\{\alpha(i_1), \beta(j_1)\}, \cdots, P\{\alpha(i_\mu), \beta(j_\mu)\}\Big\} \qquad (k = 1, \cdots, n),$$

and further define $s_k\{a, b\}$ by

$$s_k\{a, b\} = S\{\alpha_k, \beta_k\} \qquad (k = 1, \cdots, n).$$

Then it is easily seen that

$$z \equiv (\zeta_1, \cdots, \zeta_n), \quad v \equiv (v_1, \cdots, v_n), \quad \zeta_j \equiv \zeta \qquad (j = 1, \cdots, n),$$
$$v_1 \quad v, \ v_j \quad \zeta \qquad (j = 2, \cdots, n),$$
$$S_j\{a, b\} \equiv s_j\{a, b\}, \quad P_j\{a, b\} \equiv p_j\{a, b\} \qquad (j = 1, \cdots, n),$$

is a solution $z, v, S_j\{a, b\}, P_j\{a, b\}$ *of the postulates* (10.1)–(10.4) *of* § 10, *and further that in order that these be also a solution of* (10.5) *it is sufficient that*

$$i_s \leqq k, \ j_s \leqq k \qquad (k = 1, \cdots, n).$$

When the last condition is satisfied we shall call $\mathfrak{G}_D$ the *associated semigroup* of $\mathfrak{D}_n \mathfrak{U}_m$.

By changes in notation as in § 12 we define $\mathfrak{G}_C$.

17. Associated semigroups of $\mathfrak{X}_\infty \mathfrak{U}_m$ and their related $\mathfrak{X}_{\infty, \varphi} \mathfrak{U}_m$. When the order n of the matrices in $\mathfrak{X}_n \mathfrak{U}_m$ is infinite we indicate this as above. Of all associated semigroups of $\mathfrak{X}_n \mathfrak{U}_m$, two are of the first importance for algebraic arithmetic. One refers to $\mathfrak{X} = \mathfrak{C}$, the other to $\mathfrak{X} = \mathfrak{D}$, and these lead respectively to additive and multiplicative algebraic arithmetic. There is also an extremely useful variant of the first, which will be defined presently.

Let $a \equiv (\alpha_0, \alpha_1, \alpha_2, \cdots)$, $b \equiv (\beta_0, \beta_1, \beta_2, \cdots)$ be any two equal or distinct elements of $\mathfrak{C}_\infty \mathfrak{U}_m$. Then *a solution of the postulate system for* S_j, P_j *in* § 12 *is*

(17.1) $S_j\{a, b\} \equiv S\{\alpha_j, \beta_j\}$,

(17.2) $P_j\{a, b\} \equiv S\Big\{P\{\alpha_0, \beta_j\},\ P\{\alpha_1, \beta_{j-1}\}, \cdots, P\{\alpha_j, \beta_0\}\Big\}$,

for $j = 0, 1, 2, \cdots$, and the zero $z \equiv (\zeta, \zeta, \zeta, \cdots)$, the unity $u \equiv (v, \zeta, \zeta, \zeta, \cdots)$ where, (as in § 2), ζ, $v \equiv$ the zero, unity in $\mathfrak{U}_m$.

Let $a \equiv (\alpha_1, \alpha_2, \alpha_3, \cdots)$, $b \equiv (\beta_1, \beta_2, \beta_3, \cdots)$ be any two equal or distinct elements of $\mathfrak{D}_\infty \mathfrak{U}_m$. Then *a solution of the postulate system for* S_j, P_j *in* § 10 *is*

(17.3) $S_j\{a, b\} \equiv S\{\alpha_j, \beta_j\}$,

(17.4) $P_j\{a, b\} \equiv S\Big\{P_j\{\alpha_{d_1}, \beta_{j/d_1}\},\ P\{\alpha_{d_2}, \beta_{j/d_2}\}, \cdots, P\{\alpha_{d_r}, \beta_{j/d_r}\}\Big\}$,

for $j = 1, 2, 3, \cdots$, *where* $d_k (k = 1, \cdots, r)$ *are all the divisors* > 0 *of* j (*including* $1, j$); the zero, unity are $z \equiv (\zeta, \zeta, \zeta, \cdots)$, $u \equiv (v, \zeta, \zeta, \cdots)$.

That these are indeed solutions can be verified by direct substitution into the postulate systems. Indicate the solutions (17.1), (17.2) and (17.3), (17.4) by $\mathfrak{S}_C$, $\mathfrak{S}_D$ respectively.

Consider first $\mathfrak{S}_C$. Let τ be a parameter in $\mathfrak{U}_m$ (whose unity is v, and in which S, P are addition, multiplication). Write

$$\tau_0 \equiv v,\ \tau_k \equiv P\{\tau, \tau, \cdots, \tau\} \qquad (k = 1, 2, \cdots),$$

the τ in the P product τ_k being repeated precisely k times. Then *the elements* τ_j *of* $t \equiv (\tau_0, \tau_1, \tau_2, \cdots)$ *furnish an instance* (in the case of n infinite as here) *of* $\mathfrak{G}_C$ *in* § 16, *and we have now*

(17.5) $$P\{\tau_i, \tau_j\} = \tau_{i+j}$$

for i, j *any integers* > 0. *Hence, if* $a \equiv (\alpha_0, \alpha_1, \alpha_2, \cdots)$ *is any element of* $\mathfrak{C}_\infty \mathfrak{U}_m$ *we have*

(17.6) $\varphi_C\{a, t\} \equiv S\Big\{P\{\alpha_0, \tau_0\},\ P\{\alpha_1, \tau_1\},\ P\{\alpha_2, \tau_2\}, \cdots\Big\}$

as the form of any element of $\mathfrak{C}_{\infty, \varphi}\ \mathfrak{U}_m$ (see §§ 13–15) *in the solution* $\mathfrak{S}_C$. Applied to (17.6) the theory in §§ 13–15

is the direct generalization to $\mathfrak{U}_m$ of the algebraic theory of power series in $\mathfrak{F}_c$, reductions of all functions of elements of $\mathfrak{C}_{\infty,q}\ \mathfrak{U}_m$ to the form (17.6) being made by repeated application of (17.5) to all P products of parameters τ_j $(j = 0, 1, 2, \cdots)$ occuring in the functions.

Next, consider $\mathfrak{S}_D$. Let now the θ_j $(j = 1, 2, 3, \cdots)$ be parameters in $\mathfrak{U}_m$, and let

$$n = p_1^{k_1}\, p_2^{k_2} \cdots p_s^{k_s}\ (k_j > 0,\ j = 1, \cdots, s)$$

be the resolution of $n > 1$ into a product of powers of distinct rational primes. For $p_j > 1$ prime, and $k > 0$ an integer, write $\theta_p^k \quad \{\theta_p, \theta_p, \cdots, \theta_p\}$, the θ_p in the last being repeated precisely k times. For n as above let

$$\tau_n \equiv P\{\theta_{p_1}^{k_1}, \theta_{p_2}^{k_2}, \cdots, \theta_{p_s}^{k_s}\}, \qquad \tau_1 \equiv \theta_1 \equiv v.$$

Then *the elements* τ_j *of* $t \equiv (\tau_1, \tau_2, \tau_3, \cdots)$ *give an instance* (n infinite) *of* $\mathfrak{G}_D$ *in* § 16, *and if* $a \equiv (\alpha_1, \alpha_2, \alpha_3, \cdots)$ *is any element of* $\mathfrak{D}_\infty\ \mathfrak{U}_m$, *then the form of any element* $\varphi_D\{a, t\}$ *of* $\mathfrak{D}_{\infty,q}\ \mathfrak{U}_m$ *in the solution* $\mathfrak{S}_D$ *is*

$$(17.7) \quad \varphi_D\{a, t\} \equiv S\{P\{\alpha_1, \tau_1\},\ P\{\alpha_2, \tau_2\},\ P\{\alpha_3, \tau_3\}, \cdots,\}$$

and reductions in $\mathfrak{D}_{\infty,q}\ \mathfrak{U}_m$ *are made to the form* (17.7) *by means of*

$$(17.8) \qquad P\{\tau_i, \tau_j\} = \tau_{ij},$$

where i, j *are any integers* ≥ 1, *and* ij *in the last is the product of* i *and* j (not a double suffix). Applied to §§ 13–15, (17.7) is the direct generalization to $\mathfrak{U}_m$ of the algebra of common Dirichlet series in F_c.

Since in each of $\mathfrak{X}_\infty\ \mathfrak{U}_m$, $\mathfrak{X} = \mathfrak{C}, \mathfrak{D}$, the order of each element (= matrix) is infinite, it follows that both of these varieties contain an infinity of irregular elements, since any irregular element of $\mathfrak{U}_m$ may occupy the first k $(k = 1, 2, \cdots)$ places in a matrix. Hence *each of* $\mathfrak{X}_{\infty,q}\ \mathfrak{U}_m$ *is an instance of* $\mathfrak{J}\mathfrak{F}$, *and similarly therefore for each of* $\mathfrak{X}_{\infty,\varphi}\ \mathfrak{U}_m$. This

holds wether $\mathfrak{U}_m$ is regular or irregular, and hence in particular it holds in the instances $\mathfrak{F}_j$ $(j = c, r)$ of $\mathfrak{U}$.

18. Varieties $\mathfrak{U}_m$ over $\mathfrak{A}$. The entire preceding theory can be generalized by *taking* $\mathfrak{U}_m$ *over* $\mathfrak{A}$, the postulates for the italicized process being obtained by obvious slight modifications from the like for an algebra over a field as in Dickson, *Algebras and their Arithmetics*, § 4. We shall need in particular the postulates for scalar multiplication (the elements of $\mathfrak{A}$ being the scalars) of elements of $\mathfrak{U}_m$ with respect to $\mathfrak{A}$, and we may assume these to have been stated from Dickson. If α_j is in $\mathfrak{U}_m$, and g is in the instance $\mathfrak{F}_r$ of $\mathfrak{A}$, the scalar product of g, α_j is written $g\alpha_j$.

To illustrate the numerous possibilities we outline a specially useful generalization, $\mathfrak{B}_\infty\,\mathfrak{U}_m$ and its associated $\mathfrak{B}_{\infty,q}\,\mathfrak{U}_m$, of $\mathfrak{C}_\infty\,\mathfrak{U}_m$ and its associated $\mathfrak{C}_{\infty,q}\,\mathfrak{U}_m$, by extending the latter to $\mathfrak{U}_m$ over $\mathfrak{F}_r$.

The elements $\neq t$ of $\mathfrak{B}_\infty\,\mathfrak{U}_m$ are indicated by accenting those of $\mathfrak{C}_\infty\,\mathfrak{U}_m$, thus

$$a' \equiv (\alpha'_0, \alpha'_1, \cdots), \qquad b' \equiv (\beta'_0, \beta'_1, \cdots);$$

and if $d' \equiv (\delta'_0, \delta'_1, \cdots)$ is any element of $\mathfrak{B}_\infty\,\mathfrak{U}_m$, the δ'_j $(j = 0, 1, \cdots)$ are in $\mathfrak{U}'_m$, the latter being $\mathfrak{U}_m$ taken over $\mathfrak{F}_r$. Specifically, $\mathfrak{B}_\infty\,\mathfrak{U}_m$ *is that instance of* $\mathfrak{C}_\infty\,\mathfrak{U}'_m$ *in which* $\delta'_j \equiv \delta_j/j!$ $(j = 0, 1, \cdots)$, *where* $d' \equiv (\delta'_0, \delta'_1, \cdots)$ *is any element of* $\mathfrak{B}_\infty\,\mathfrak{U}_m$ *and* $d \equiv (\delta_0, \delta_1, \cdots)$ *is any element of* $\mathfrak{C}_\infty\,\mathfrak{U}_m$; $t \equiv (\tau_0, \tau_1, \cdots)$ *is the parameter in* $\mathfrak{B}_{\infty,q}\,\mathfrak{U}_m$ *and is identical with the parameter* t *in* $\mathfrak{C}_{\infty,q}\,\mathfrak{U}_m$.

Addition, multiplication in $\mathfrak{B}_\infty\,\mathfrak{U}_m$ are indicated by S_B, P_B, and are defined as follows. Let $a' \equiv (\alpha'_0, \alpha'_1, \cdots)$, $b' \equiv (\beta'_0, \beta'_1, \cdots)$ be any elements of $\mathfrak{B}_\infty\,\mathfrak{U}_m$. Their *sum*, $S_B\{a', b'\}$ is the element s' of $\mathfrak{B}_\infty\,\mathfrak{U}_m$, where, for $j = 0, 1, \cdots$, $s' \equiv (\sigma'_0, \sigma'_1, \cdots)$, $\sigma'_j \equiv \sigma_j/j!$, $\sigma_j \equiv S\{\alpha_j, \beta_j\}$; their *product* $P_B\{a', b'\}$ is the element p' of $\mathfrak{B}_\infty\,\mathfrak{U}_m$, where for $j = 0, 1, \cdots$,

$$p' \equiv (\pi'_0, \pi'_1, \cdots), \qquad \pi'_j \equiv \pi_j/j!,$$

$$\pi_j \equiv S\big\{(j,0)\,P\{\alpha_j, \beta_0\},\ (j,1)\,P_j\{\alpha_{j-1}, \beta_1\},\ \cdots,\ (j,j)\,P\{\alpha_0, \beta_j\}\big\},$$

in which $0! = 1$, and (j, r) the coefficient of x^r in $(1+x)^j$.

With these definitions it is easily seen that $\mathfrak{B}_\infty \mathfrak{U}_m$ and $\mathfrak{B}_{\infty,q} \mathfrak{U}_m$ are an instance of $\mathfrak{C}_\infty \mathfrak{U}'_m$, $\mathfrak{C}_{\infty,q} \mathfrak{U}'_m$, where $\mathfrak{U}'_m$ is $\mathfrak{U}_m$ taken over $\mathfrak{F}_r$. When $\mathfrak{U}_m$ is replaced by its instance $\mathfrak{F}_c$, the instance $\mathfrak{B}_{\infty,q} \mathfrak{F}_c$ of the above is identical with the powerful symbolic or umbral calculus invented by Blissard and Lucas, which is indispensable in the algebraic analysis of sequences of numbers or functions.

THE IRREGULAR FIELDS $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ ASSOCIATED WITH $\mathfrak{A}$, §§ 19–23

19. Instances of the foregoing theory for $\mathfrak{U}_1$. When $m = 1$, $\mathfrak{U}_m$ $\mathfrak{A}$, and there is but the single irregular element 0. The unity is 1 (see § 1); and S, P are now in a more familiar form, $S\{\alpha_j, \beta_j\} = \alpha_j + \beta_j$, $P\{\alpha_j, \beta_j\} = \alpha_j \beta_j$, where α_j, β_j are any elements of $\mathfrak{A}$. We shall write

$$\mathfrak{Y}_\infty \mathfrak{A} \equiv \mathfrak{Y} \quad (\mathfrak{Y} \equiv \mathfrak{B}, \mathfrak{C}, \mathfrak{D}), \tag{19}$$

so that $\mathfrak{Y}$ is the instance when $m = 1$ of $\mathfrak{Y}_\infty \mathfrak{U}_m$, and similarly for $\mathfrak{Y}_{\infty,q} \mathfrak{A}$. Addition, multiplication in $\mathfrak{Y}$ are indicated as before, S_Y, P_Y. As the three irregular fields (19) are of particular importance in algebraic arithmetic it will be convenient to have short summaries of them in the simplified forms consequent upon taking $m = 1$ in $\mathfrak{U}_1$. These are written down immediately from the corresponding general developments (m arbitrary) in §§ 11, 12 (with $n = \infty$ therein), 17, 18 and § 15. Elements of $\mathfrak{A}$ are denoted by $\alpha_j, \beta_j, \gamma_j, \cdots$ and the τ, τ_j are parameters in $\mathfrak{A}$.

20. The irregular field $\mathfrak{C}$. The elements of $\mathfrak{C}$ are $a \equiv (\alpha_0, \alpha_1, \cdots)$, $b \equiv (\beta_0, \beta_1, \cdots)$, $c \equiv (\gamma_0, \gamma_1, \cdots)$, $\cdots$; the parameter $t \equiv (\tau_0, \tau_1, \cdots) \equiv (1, \tau, \tau^2, \cdots)$; the zero, unity in $\mathfrak{C}$ are $z \equiv (0, 0, 0, \cdots)$, $u \equiv (1, 0, 0, \cdots)$; addition, multiplication are defined by $S_C\{a, b\} = s$, $P_C\{a, b\} = p$, where $s \equiv (\sigma_0, \sigma_1, \cdots)$, $p \equiv (\pi_0, \pi_1, \cdots)$, and

$$\sigma_j \equiv \alpha_j + \beta_j, \quad \pi_j \equiv \alpha_j \beta_0 + \alpha_{j-1} \beta_1 + \cdots + \alpha_1 \beta_{j-1} + \alpha_0 \beta_j \quad (j = 0, 1, \cdots);$$

the associated function $\varphi_C\{a, t\}$ (of a for the parameter t) is $\varphi_C\{a, t\} \equiv \sum_0^\infty \alpha_n \tau^n$. If

$$I(x, y, \cdots, v) \equiv 0 \tag{20.1}$$

is an identity in elements $x, y, \cdots, v$ of $\mathfrak{A}$ then, provided no divisor be irregular, (20.1) is an identity when $x, y, \cdots, v$ are interpreted as elements of $\mathfrak{C}$, and the $\mathfrak{C}$ form of (20.1) can be inferred from the $\mathfrak{A}$ form from the abstractly identical relation

$$I(\varphi_C\{x, t\}, \varphi_C\{y, t\}, \cdots, \varphi_C\{v, t\}) \equiv \varphi_C\{z, t\} \tag{20.2}$$

in $\mathfrak{C}_{\infty, \varphi}\mathfrak{A}$ by equating to 0 the coefficients of $\tau^n (n = 0, 1, \cdots)$. Associated functions in $\mathfrak{C}$ may be called *power series* (they are such in the usual sense only when $\mathfrak{A}$ is replaced by its instances $\mathfrak{F}_c$, $\mathfrak{F}_r$).

21. The irregular field $\mathfrak{D}$. The elements of $\mathfrak{D}$ are $a = (\alpha_1, \alpha_2, \cdots)$, $b = (\beta_1, \beta_2, \cdots)$, $c = (\gamma_1, \gamma_2, \cdots)$, $\cdots$; the parameter $t \equiv (\tau_1, \tau_2, \cdots)$ where

$$\tau_n \equiv \theta_{p_1}^{k_1} \theta_{p_2}^{k_2} \cdots \theta_{p_s}^{k_s}, \qquad \tau_1 \equiv \theta_1 = 1$$

the n, $p_j (j = 1, \cdots, s)$ being as in § 17, and the θ_q, where q runs through all primes ≥ 1, being independent parameters in $\mathfrak{A}$. The zero, unity in $\mathfrak{D}$ are $z \equiv (0, 0, \cdots)$, $u \equiv (1, 0, 0, \cdots)$; addition, multiplication in $\mathfrak{D}$ are defined by $S_D\{a, b\} = s$, $P_D\{a, b\} \equiv p$, where $s \equiv (\sigma_1, \sigma_2, \cdots)$, $p \equiv (\pi_1, \pi_2, \cdots)$, and $\sigma_j \equiv \alpha_j + \beta_j$, $\pi_j \equiv \sum \alpha_r \beta_s (rs = j, r, s \geq 1)$ $(j = 1, 2, \cdots)$, (the sum in the last refers to all pairs (r, s) of conjugate divisors r, s of j); the associated function $\varphi_D\{a, t\} = \sum_1^\infty \alpha_n \tau_n$, and $\tau_m \tau_n = \tau_{mn}$ for m, n any integers > 0. In precisely the same way as in $\mathfrak{C}$ with respect to (20.1), (20.2), we have an abstractly identical conclusion in $\mathfrak{D}$ on equating coefficients of $\tau_n (n = 1, 2, \cdots)$.

22. The irregular field $\mathfrak{B}$. It will be sufficient to state the algorithm of $\mathfrak{B}$, which follows from §§ 18, 20, in relation to the associated functions $\varphi_B\{a, t\}$, $a = (\alpha_0, \alpha_1, \cdots)$,

$$\varphi_B\{a, t\} = \sum_0^\infty \alpha_n \tau^n / n!.$$

Raise suffixes of elements of $\mathfrak{A}$ thus $\alpha_n \qquad \alpha^n$, symbolic exponents, as in α^n, being lowered after completion of operations in $\mathfrak{B}$. Then, for $r = 0, 1, \cdots, j$, we write

$$(\alpha+\beta)^n \equiv \sum (j, r)\, \alpha^{j-r}\beta^r \equiv \sum (j, r)\, \alpha_{j-r}\beta_r,$$

where (j, r) is as in § 18, and symbolically

$$\varphi_B\{a, t\} \equiv e^{\alpha\tau} \equiv \exp \alpha\tau.$$

Precisely as in $\mathfrak{F}_c$ it follows that

$$\exp \alpha\tau \cdot \exp \beta\tau = \exp (\alpha+\beta)\tau,$$

the indicated multiplication on the left being in $\mathfrak{B}_{\infty,\varphi}\mathfrak{A}$. If in this $b = a$, one of the equal *umbrae* β, α is replaced by a symbol (umbra) different from α, say β, until after the completion of all reductions in $\mathfrak{B}_{\infty,\varphi}\mathfrak{A}$. Addition in the last being defined by

$$\exp \alpha\tau + \exp \beta\tau \equiv \exp \gamma\tau, \quad \gamma_j \equiv \alpha_j + \beta_j \qquad (j = 0, 1, \cdots),$$

we again have in $\mathfrak{B}$ a conclusion abstractly identical with that in $\mathfrak{C}$ regarding (20.1), (20.2). In $\mathfrak{B}$ the associated functions $\varphi_B\{a, t\} \qquad \exp \alpha\tau$ have algebraic properties abstractly identical with those of the exponential function in $\mathfrak{F}_c$, and hence the derivation of relations in $\mathfrak{B}$ is reduced to the transformation of identities between exponentials in $\mathfrak{F}_c$ (or in $\mathfrak{A}$). Associated functions in $\mathfrak{B}$ may be called *exponential series*, and in an obvious way we define, by means of sums and differences, etc., of such functions, the *circular functions in* $\mathfrak{A}$.

23. Differentation and integration in $\mathfrak{C}$. An identity in $\mathfrak{C}$ may be transformed in an infinity of ways by $\mathfrak{C}$ operations to produce new identities in $\mathfrak{C}$. For example, from $a = b$ in $\mathfrak{C}$ we infer $P\{a, c\} = P\{b, c\}$. As we shall see later, in discussing $\mathfrak{E}$, even the most trivial $\mathfrak{C}$ identities yield interesting and by no means obvious relations between functions of divisors. An unlimited number of such relations flow from the operations ∂ (differentiation) and ∂^{-1} (inte-

gration) in $\mathfrak{C}$, which are defined as follows. Take $\mathfrak{A}$ over $\mathfrak{F}_r$, getting $\mathfrak{A}'$, $\mathfrak{C}'$ (see § 18),

$$a \equiv (\alpha_0, \alpha_1, \cdots), \quad a' \equiv (\alpha_0', \alpha_1', \cdots), \quad a'' \equiv (\alpha_0'', \alpha_1'', \cdots)$$

in which the α_j', α_j'' are defined by

$$\alpha_j' = (j+1)\alpha_{j+1} \ (j = 0, 1, \cdots); \ \alpha_0'' = 0, \ \alpha_j'' = \alpha_{j-1}/j \ (j = 1, 2, \cdots).$$

Then we shall write (∂^r, ∂^{-r} are operators)

$$a' \equiv \partial a, \quad a'' \equiv \partial^{-1} a, \quad \partial^0 a \equiv a, \quad \partial \equiv \partial^1,$$
$$\partial^r a \equiv \partial(\partial^{r-1} a), \quad \partial^{-r} a \equiv \partial^{-1}(\partial^{-r+1} a) \ (r = 0, 1, \cdots),$$

and therefore

$$\partial^r(\partial^{-r} a) = \partial^{-r}(\partial^r a) = a.$$

Hence, if x, y are in $\mathfrak{C}$ (or $\mathfrak{C}'$), and if for the moment we indicate $\mathfrak{C}$ operations by the same notations $x+y$, xy, etc., as those for the abstractly identical operations in $\mathfrak{A}$, we have

$$\partial(x+y) = \partial x + \partial y, \quad \partial(xy) = x\partial y + y\partial x,$$
$$\partial(x/y) = (y\partial x - x\partial y)/y^2, \quad \partial x^n = n x^{n-1} \partial x,$$

and $\partial(cx) = c\partial x$, where c is scalar, precisely as in the calculus in $\mathfrak{F}_c$. It is unnecessary to verify these as they are implied by § 20. As a frequently useful consequence, (20.2) may be differentiated or integrated with respect to t as if it were an analytic relation between convergent power series capable of termwise differentiation and integration.

THE PARTITIONS OF A MATRIX, §§ 24–26

24. Coprime matrices, conjoints. For immediate use in $\mathfrak{P}$, discussed in the next chapter, we continue with certain properties of matrices as defined in §§ 8–9. The elements (matrices) of a set of matric variables having no variable (scalar) in common are said to be *coprime*. If ξ, η are coprime matric variables, and c is a scalar, $c\xi$, $c\eta$ are coprime.

From the n independent variables x_j of $\xi \equiv (x_1, \cdots, x_n)$ can be constructed precisely $2^n - 1$ matric variables of orders

$\leqq n$ (since by §§ 8 9 it is presupposed that all matrices are normal). Let ξ_j $(j = 1, \cdots, 2^n - 1)$ be these matric variables, and let the c, c_j denote scalar constants $\neq 0$; also let $\xi_\alpha, \xi_\beta, \cdots, \xi_\gamma$ be coprime elements of the set ξ_j $(j = 1, \cdots, 2^n - 1)$, all of whose elements together are the set x_i $(i = 1, \cdots, n)$ of the elements of ξ. Then ξ is called the *conjoint* of $\xi_\alpha, \xi_\beta, \cdots, \xi_\gamma$ and we write

$$\xi = \xi_\alpha + \xi_\beta + \cdots + \xi_\gamma.$$

The conjoint η of $c_\alpha \xi_\alpha, c_\beta \xi_\beta, \cdots, c_\gamma \xi_\gamma$ is

$$\eta = c_\alpha \xi_\alpha + c_\beta \xi_\beta + \cdots + c_\gamma \xi_\gamma,$$

which is defined by the preceding since the $c_\delta \xi_\delta (\delta = \alpha, \beta, \cdots, \gamma)$ are a coprime set. Non-coprime matrices cannot be conjoined. Conjunction, which in $\mathfrak{P}$ replaces the usual addition of matrices in $\mathfrak{A}$, is analogous to logical addition; it is commutative and associative.

The conjoint of $-c_\alpha \xi_\alpha, -c_\beta \xi_\beta, \cdots, -c_\gamma \xi_\gamma$ is $-\eta$. When convenient conjoints are enclosed in parentheses,

$$-\eta = -(c_\alpha \xi_\alpha + c_\beta \xi_\beta + \cdots + c_\gamma \xi_\gamma),$$

and evidently such expressions obey laws abstractly identical with those for the like in $\mathfrak{A}$. Thus, for example, ξ, η, θ being coprime, we have

$$-\xi + \eta + \theta = -(\xi - \eta - \theta) = -\xi - (-\eta - \theta).$$

The *zero conjoint* (0) (corresponding to the null class) is the matrix having no elements; $(0) \neq (0)_n$. The *matric product* of any number of matric variables is the matric variable whose elements are all the variables common to all the factors; the matric sum is the matric variable consisting of all the variables (each taken once only) in all the factors. These definitions are included only for completeness; they are not required in $\mathfrak{P}$ but are useful in the theory of arithmetical structure (which will be briefly sketched in the concluding chapter).

25. Residues in a module. Let α_i $(i = 1, 2, \cdots)$ be elements of a module $\mathfrak{M}$. Then, 0 being in $\mathfrak{M}$, $\alpha_i - \alpha_i = 0 = 0\alpha_i = \alpha_i 0$ for each α_i in $\mathfrak{M}$, and any element $\alpha \neq 0$ of $\mathfrak{M}$ is of the form

$$\alpha = k_a\alpha_a + k_b\alpha_b + \cdots + k_c\alpha_c,$$

where the k's are rational integers $\neq 0$ and the α's are distinct.

Replace each k_j by its least positive residue mod m; call the resulting element of $\mathfrak{M}$ the *positive residue* of α mod m, and write

$$\alpha \equiv m_a\alpha_a + m_b\alpha_b + \cdots + m_c\alpha_c \bmod m.$$

Each element of $\mathfrak{M}$ has precisely one positive residue mod m. The set $\mathfrak{M}_m$ of all positive residues mod m of elements of $\mathfrak{M}$ is a module, say $\mathfrak{M}_m$. The *sum* (*difference*) of any two elements of $\mathfrak{M}_m$ is the positive residue mod m of the algebraic sum (difference) of the given elements. The last defines $\mathfrak{M}_m$. in which each element α is of the form $r_a\alpha_a + r_b\alpha_b + \cdots + r_c\alpha_c$, where $\alpha_a, \alpha_b, \cdots, \alpha_c$ are s distinct elements of $\mathfrak{M}$, and each of $r_a, r_b, \cdots, r_c$ is a definite one of $1, 2, \cdots, m-1$. Hence if $\mathfrak{M}$ has the finite basis $[\alpha_1, \cdots, \alpha_n]$, $\mathfrak{M}_m$ contains precisely $m^n - 1$ elements $\neq 0$.

Let each e_j $(j = 1, 2, \cdots, n)$ be a definite one of $1, -1$. Then, of the 2^s distinct elements of the form

$$e_a r_a \alpha_a + e_b r_b \alpha_b + \cdots + e_c r_c \alpha_c$$

of $\mathfrak{M}$, where the e's take all their possible values, precisely one, namely α, given by $e_a = e_b = \cdots = e_c = 1$ is in $\mathfrak{M}_m$. The remaining $2^s - 1$ elements of this form are called the *conjugates* in $\mathfrak{M}$ of α. Any element of $\mathfrak{M}_m$ is the positive residue of each of its conjugates in $\mathfrak{M}$. The element $\alpha_1 + \alpha_2 + \cdots + \alpha_n$ of $\mathfrak{M}_m$ whose basis is $[\alpha_1, \alpha_2, \cdots \alpha_n]$ is called the *trace* of $\mathfrak{M}_m$.

When $m = 2$, the case applicable to $\mathfrak{P}$, each element $\alpha \neq 0$ of $\mathfrak{M}_2$ is of the form $\alpha_a + \alpha_b + \cdots + \alpha_c$, where the α's are distinct, and the conjugates of α in $\mathfrak{M}$ are

$$e_a\alpha_a + e_b\alpha_b + \cdots + e_c\alpha_c \qquad (e_j = \pm 1,\ j = a, b, \cdots, c).$$

As $m = 2$ is the only instance which will be applied in detail we confine the following remarks on partitions to it.

26. Partitions in $\mathfrak{M}_2$. Let $\mu_j (j = 1, \cdots, n)$ be n coprime matric variables. Then $[\mu_1, \mu_2, \cdots, \mu_n]$ is the basis of an instance $\mathfrak{M}_2'$ of $\mathfrak{M}_2$, whose trace μ is the conjoint $\mu_1 + \mu_2 + \cdots + \mu_n$; the conjugates of μ are the $e_1\mu_1 + e_2\mu_2 + \cdots + e_n\mu_n$ $(e_j = \pm 1, j = 1, \cdots, n)$, with the exception of μ itself. Except in the case (trivial in applications) $n = 1$, $\mu =$ a scalar variable, μ can be separated into a set of conjoints in more than one way; call any such set a *partition* of μ, and let $\pi \equiv \mu_a + \mu_b + \cdots + \mu_c$ be any partition of μ.

All the π are obtained by distributing all the elements of μ in all possible ways into coprime sets, forming from these sets (normal) matrices, and taking the conjoint of each resulting set of coprime matric variables. If the order of μ_j in $[\mu_1, \cdots \mu_n]$ is ω_j $(j = 1, \cdots, n)$, μ is of order $\omega = \omega_1 + \cdots + \omega_n$, and the total number of partitions π is the number $\Pi(\omega)$ of distributions of ω different things into non-overlapping parcels—a well known function in combinatory analysis for which there is no concise or usable expression. This lack is unfortunate, as $\Pi(\omega)$, we shall see, is in a precise way an index of the generality of the general arithmetical theorems implicit in an identity between elliptic and theta functions involving precisely ω independent variables.

The set of all partitions π together with their conjugates are fundamental in the applications of periodic functions to algebraic arithmetic, and these applications are themselves instances of the algebra $\mathfrak{P}$ considered next. They also appear as basic in the applications of $\mathfrak{B}$, particularly to the Bernoullian numbers and functions and their generalizations to allied functions of n complex variables, but we shall not have space to go into these in detail.

CHAPTER II

THE ALGEBRA $\mathfrak{P}$ OF PARITY

ABSOLUTE AND RELATIVE PARITY, §§ 1–6

1. Origin of $\mathfrak{P}$. Functions admitting expansions into sums of powers of linear homogeneous functions of their arguments, also certain other *types* (in a technical sense) of functions to be noticed in the next chapter, give rise in their applications to algebraic arithmetic to the interesting algebra $\mathfrak{P}$ of parity. Conversely, for the full and efficient development of the algebraic arithmetic implicit in the analytic theory of such functions, for example the elliptic and the theta of $n \geq 1$ arguments, $\mathfrak{P}$ is essential. We shall therefore consider it in some detail. By itself $\mathfrak{P}$ is an interesting example of the abstract identity of the simultaneous solutions of several overlapping systems of postulates.

In the following presentation of the main outlines of $\mathfrak{P}$ the reasoning is necessarily of a somewhat abstract character, as the $\mathfrak{P}$ theorems relate to functions which are entirely arbitrary except in two respects: each function has parity, as defined presently, and each takes a single definite value for each set of integral values of all its arguments. Hence in particular all assumptions on the final functions as to continuity, differentiability, or expansibility into series of any type whatever — in fact all the customary machinery of analysis except uniformity with respect to integral arguments — must be avoided in the proofs. The point concerning assumptions as to expansibility, particularly into trigonometric series, is to be specially noticed, as it is by such excluded means that an exceedingly simple and equally fallacious method of "proving" certain of the principal theorems in their unrestricted forms is at once suggested. This very absence of restrictions upon the functions in $\mathfrak{P}$ is the

essential and sometimes rather elusive crux in the proofs of those theorems concerning the functions which are most frequently used in subsequent applications to algebraic arithmetic.

As the theorems of $\mathfrak{P}$ are ultimately finite identities between matric variables whose elements are rational integers, we shall avoid so far as is feasible without undue elaboration all reference to infinite processes, although certain of the basic lemmas for specific applications, for example those connecting $\mathfrak{P}$ with elliptic functions, can be obtained by such means. The final arithmetic being algebraic and not analytic, it is fitting that a minimum of analysis be employed in obtaining the fundamental theorems. In the last step connecting $\mathfrak{P}$ with the algebraic arithmetic of the common periodic functions it is sufficient (but not necessary) to assume only the power series for the sine and cosine. The complete $\mathfrak{P}$, abstract structure and instances, is a novel example of the application of algebra to analysis with the object of obtaining applications of analysis to arithmetic; the algebra in turn can be replaced by elementary identities in rational arithmetic, so that in the end we have applications of rational arithmetic to analysis instead of the more usual reverse.

In following the development of $\mathfrak{P}$ with a view to possible generalizations, some may be interested in observing that the elemental, generative fact underlying the entire theory of parity in all of its ramifications—which are many—is the protean one that any rational integer when divided by 2 yields one or other of the positive remainders 0, 1. Hence, since the theory of elliptic functions is contained as an instance in some of the simpler identities in $\mathfrak{P}$, all of which can be proved independently by elementary arithmetic, it follows that double periodicity, etc., can be traced to the same simple source. There is a generalization of $\mathfrak{P}$ to moduli $n > 2$, and the like applies to $\mathfrak{B}$ of the preceding chapter, in which the units of any algebraic number field replace the units ± 1 of rational arithmetic in the case $n > 2$, and there is a further

generalization with respect to any algebraic number field. The analytic functions to which the last extension could be applied with profit to arithmetic have yet to be investigated for $\mathfrak{P}$; they can be easily constructed in the form appropriate for $\mathfrak{B}$. Hecke's theta formula is an instance of the type of theorem which can be applied to an extended $\mathfrak{P}$. A great desideratum for $\mathfrak{P}$ is a practicable form of the trigonometric series for the n-fold periodic functions, $n>2$. The discussion by Appell (*Acta Mathematica*, vol. 13, pp. 1–174), for $n=4$. analytically complete, abandons the problem precisely where its utility for arithmetic begins.

2. Absolute and relative parity. The definitions already stated for matrices, their functions and partitions, are presupposed. We shall develop $\mathfrak{P}$ with respect to $\mathfrak{A}$. Hence all matric variables are in $\mathfrak{A}$.

Parity is the eveness or oddness of a function with respect to its matric variables.

A function whose value remains unchanged when the matric variable z of order n is replaced by $-z$ is said to be of *even absolute parity n in z*; if the value of the function changes sign when z is replaced by $-z$, the function is of *odd absolute parity n in z*. The even, odd absolute parities just defined are written $p(n\ 0)$, $p(0\ n)$ respectively, and the absolute parity of a constant with respect to z is $p(0\ 0)$. The absolute parity of a function is the same as that of any of its constant scalar multiples.

An arbitrary function $f(z)$ of z has in general no parity. Such a function however may be written as the sum of two functions of the respective parities $p(n\ 0)$, $p(0\ n)$, where n is the order of z,

$$2f(z) = [f(z)+f(-z)]+[f(z)-f(-z)],$$

since $f(z)\pm f(-z)$ are of these respective parities, precisely as in the common instance of this for $n=1$.

Let λ_i, $\mu_j (i=1,\cdots,r;\ j=1,\cdots,s)$ be $r+s$ coprime matric variables of the respective orders a_i, b_j. Then a function f whose even absolute parity in λ_i is $p(a_i\ 0)$

$(i = 1, \cdots, r)$, and whose odd absolute parity in μ_j is $p(0 \mid b_j)$ $(j = 1, \cdots, s)$ is defined to have the *absolute parity*

$$p(a_1, \cdots, a_r \; b_1, \cdots, b_s). \tag{2.1}$$

When necessary to refer to the matric variables λ_i, μ_j, and not merely to their orders a_i, b_j, we shall say that f has the *relative parity*

$$p(\lambda_1, \cdots, \lambda_r \mid \mu_1, \cdots, \mu_s). \tag{2.2}$$

An absolute parity is a function of positive integers, a relative parity is a function of matric variables. If the odd obsolute parities are lacking, (2.1), (2.2) will be written

$$p(a_1, \cdots, a_r \mid 0), \qquad p(\lambda_1, \cdots, \lambda_r \mid); \tag{2.3}$$

similarly, if the even absolute parities are absent we write

$$p(0 \mid b_1, \cdots, b_s), \qquad p(\mid \mu_1, \cdots, \mu_s). \tag{2.4}$$

Unless otherwise evident from the context p is used exclusively to indicate parity.

Any function f of the matric variables λ_i, μ_j having the parity (2.1) or (2.2) will be written

$$f(\lambda_1, \cdots, \lambda_r \mid \mu_1, \cdots, \mu_s); \tag{2.5}$$

corresponding to (2.3) we write in the same way

$$g(\lambda_1, \cdots, \lambda_r \mid), \tag{2.6}$$

and to (2.4),

$$h(\mid \mu_1, \cdots, \mu_s). \tag{2.7}$$

In the symbols (2.1)–(2.7) the arrangement of the a_i, b_j, λ_i, μ_j is immaterial provided only that no letter passes the bar.

If in (2.1) precisely α of the a_i $(i = 1, \cdots, r)$ each $= a_1$, and precisely β of the b_j $(j = 1, \cdots, s)$ each $= b_1$, we replace all these equal a_j or b_j by a_1^α, b_1^β in (2.1) and, proceeding thus, define

$$p(a^{\alpha},\ b^{\beta}\ \cdots,\ c^{\gamma}\mid r^{\rho},\ s^{\sigma},\ \cdots,\ t^{\tau}),$$

in which $a, b, \cdots, c$ are all distinct and likewise for $r, s, \cdots, t$. In no symbol of a relative parity or of a function having parity such as (2.2)–(2.7) can any matric variable appear twice, since the λ_i, μ_j were taken coprime in the initial definition.

To avoid a possible confusion we recall that coprimality of matrices was defined for matric variables, not for their values. Thus, for example, if x, y, z, w are independent variables, the matric variables (x, y), (z, w) are coprime, although they may have an infinity of equal values (α_i, β_i) $(i = 1, 2, \cdots)$. A proposition concerning either variables or matric variables implies instances concerning values, but not conversely unless the instances refer to the set of all possible values. The latter possibility will be discussed in connection with the theory of division of parities.

In the matric variables λ_i, μ_j the functions f, g, h in (2.5)–(2.7) have by definition the absolute parities

$$(2.8)\qquad p((1^r \mid 1^s)),\qquad p((1^r \mid 0)),\qquad p((0 \mid 1^s)),$$

the double (( )) being used to distinguish these from the absolute parities

$$(2.9)\qquad p(1^r \mid 1^s),\qquad p(1^r \mid 0),\qquad p(0 \mid 1^s)$$

obtained from (2.1) when respectively

$$a_i = 1,\ b_j = 1;\quad a_i = 1,\ b_j = 0;\quad a_i = 0,\ b_j = 1,$$
$$(i = 1, \cdots, r;\quad j = 1, \cdots, s).$$

It is sometimes convenient to include $r = 0$ or $s = 0$ in $p(1^r \mid 1^s)$. We assign by convention the following meanings, $p(1^0 \mid 1^s) \equiv p(0 \mid 1^s)$, $p(1^r \mid 1^0) \equiv p(1^r \mid 0)$. Similarly for (2.8).

Thus (2.9) is the special case of (2.8) in which the λ_i, μ_j $(i = 1, \cdots, r;\ j = 1, \cdots, s)$ are all of order 1, and $p(1^r \mid 1^s)$ is the absolute parity of a function of precisely $r + s$ independent variables, even in each of r of them and odd in the rest; $p(1^r \mid 0)$ is the absolute parity of a function of

precisely r independent variables, even in each; $p(0 \mid 1^s)$ is the absolute parity of a function of precisely s independent variables, odd in each. Again, $p(r \mid 0)$ is the absolute parity of a function of precisely r independent variables, even in all r simultaneously, and similarly for $p(0 \mid s)$ and an s-fold odd function; in the matric variables these have the respective absolute parities $p((1 \mid 0))$, $p((0 \mid 1))$.

An extension of these concepts is important shortly. Let λ_i, μ_j in (2.5) be partitioned into a'_i, b'_j matric variables $(i = 1, \cdots, r;\ j = 1, \cdots, s)$. Then the absolute parities of f, g, h in (2.5)–(2.7) in the $a'_1 + \cdots + a'_r + b'_1 + \cdots + b'_s$ matric variables occuring in the partitions will be indicated thus,

$$\begin{gathered} p((a'_1, \cdots, a'_r \mid b'_1, \cdots, b'_s)), \\ p((a'_1, \cdots, a'_r \mid 0)),\ p((0 \mid b'_1, \cdots, b'_s)). \end{gathered} \tag{2.10}$$

This merely defines the symbols (2.10); their significance will appear as we proceed. When $a'_i = a_i$, $b'_j = b_j$ $(i = 1, \cdots, r;\ j = 1, \cdots, s)$, (2.10) becomes identical with (2.1) and its subcases. As an example of (2.10), let λ, μ, ν be coprime matric variables of the respective orders l, m, n. Then $p((2 \mid 1))$ is the absolute parity of $f(\lambda + \mu \mid \nu)$ in λ, μ, ν, while in the variables (scalar elements of λ, μ, ν) the absolute parity is $p(l + m \mid n)$.

3. Absolute parity of a relative parity. As before let λ_i, μ_j be coprime matric variables of the respective orders a_i, b_j and let the u_i, v_j be constant scalars. Then by § 2,

$$f(\lambda_1, \cdots, \lambda_r \mid \mu_i, \cdots, \mu_s),\quad f(u_1\lambda_1, \cdots, u_r\lambda_r \mid v_1\mu_1, \cdots, v_s\mu_s)$$

have the same absolute parity stated in (2.1); in the matric variables they have the same absolute parity $p((1^r \mid 1^s))$. Considering the relative parity

$$p(u_1\lambda_1, \cdots, u_r\lambda_r \mid v_1\mu_1, \cdots, v_s\mu_s)$$

of the second as a function of the matric variables we assign to it the absolute parity $p((1^r \mid 1^s))$. This accords with § 2. In particular then, for $i = 1, \cdots, r$, $j = 1, \cdots, s$,

$$p(\lambda_1, \cdots, -\lambda_i, \cdots, \lambda_r | \mu_1, \cdots, \mu_s) = p(\lambda_1, \cdots, \lambda_i, \cdots, \lambda_r | \mu_1, \cdots, \mu_s),$$
$$p(\lambda_1, \cdots, \lambda_r | \mu_1, \cdots, -\mu_j, \cdots, \mu_s) = -p(\lambda_1, \cdots, \lambda_r | \mu_1, \cdots, \mu_j, \cdots, \mu_s).$$

4. **Order, degree of a function having parity.** These are fundamental in $\mathfrak{P}$ and in its applications, particularly to the elliptic and theta functions. Referring to (2.5) we write now

$$\delta_0 \equiv r, \qquad \delta_1 \equiv s, \qquad \delta \equiv \delta_0 + \delta_1,$$

and call these the *even degree*, the *odd degree*, and the *degree* respectively of f; we also define

$$\omega_0 \equiv \sum_{i=1}^{r} a_i, \qquad \omega_1 \equiv \sum_{j=1}^{s} b_j, \quad \omega \equiv \omega_0 + \omega_1$$

to be the *even order*, the *odd order*, and the *order* respectively of f. Similarly, with obvious modifications for g, h in (2.6), (2.7); for example, the even order of h is zero.

5. **Statement of two theorems.** The import of the preceding definitions will be plain from two theorems in $\mathfrak{P}$ which will later be obtained as very special cases of a general theorem which it is the object of the algebras $\mathfrak{T}$, $\mathfrak{R}_q$, introduced in a moment, to derive and reduce to a simple algorithm. The following will be recognized as further extensions of the familiar theorem which expresses a function of one variable as the sum of an even and an odd function—which we have already extended in one direction to $n > 1$ variables.

(5.1) *An arbitrary function of ω independent variables is the sum of 2^ω functions having absolute parities of the forms $p(1^a | 1^b)$, where $a + b = \omega$, and the complete statement of this which gives the number of functions of the fixed parity $p(1^a | 1^b)$, a, b constant, in the sum, is abstractly identical with De Moivre's theorem in $\mathfrak{F}_c$.*

This follows from another for which we shall have more frequent use.

(5.2) *Any function having the absolute parity $p(a_1, \cdots, a_r | b_1, \cdots, b_s)$, of order ω and degree δ, is the sum of $2^{\omega - \delta}$ properly chosen*

functions whose absolute parities are all of the type $p(1^a\ 1^b)$, *where* $a+b=\omega$, *and the complete statement of this which gives the sum is abstractly identical with the formulas in* $\mathfrak{F}_c$ *for the decomposition of a product of* r *cosines and* s *sines into a sum, and the addition theorems for* ω *arguments of the sine or cosine according as* s *is odd or even.*

The generalization of (5.2) refers to functions having the absolute parity $p((a'_1, \cdots, a'_r\ b'_1, \cdots, b'_s))$ and becomes identical with (5.2) when $a'_i = a_i$, $b'_j = b_j$ $(i = 1, \cdots, r;\ j = 1, \cdots, s)$. By considering the set of all partitions of the trace

$$\nu = \lambda_1 + \cdots + \lambda_r + \mu_1 + \cdots + \mu_s,$$

and applying the generalized (5.2) to $f(\nu\ )$, $f(\ \nu)$, we shall later obtain all the general arithmetical formulas (involving functions arbitrary beyond their parities) implicit in any identity between elliptic and theta functions, or either alone, in which precisely ω independent variables are involved, where ω is the order of ν. Thus the consequences of what is next developed are far reaching. Corresponding to the generalization of (5.2) there is an immediate extension of (5.1) to entirely arbitrary functions expressed as sums of functions having parities $p((1^a\ 1^b))$, but as this is less useful than the others we shall omit it.

6. The semigroup of coprime relative parities. The members of a set of relative parities having no matric variable in common are called *coprime*; a matric variable and its constant scalar multiples are not distinguished in this definition. Thus $p(\lambda\ )$, $p(\ -\lambda)$ are not coprime. Multiplication for non-coprime parities is not defined.

Let f, g, h be functions arbitrary beyond the respective relative parities implied by their notations,

$$f \equiv f(\lambda_1, \cdots, \lambda_r \mid \mu_1, \cdots, \mu_s), \quad g \equiv g(\varrho_1, \cdots, \varrho_t \mid \sigma_1, \cdots, \sigma_u),$$
$$h \equiv h(\lambda_1, \cdots, \lambda_r,\ \varrho_1, \cdots, \varrho_t \mid \mu_1, \cdots, \mu_s,\ \sigma_1, \cdots, \sigma_u),$$

where $\lambda_1, \cdots, \lambda_r,\ \mu_1, \cdots, \mu_s,\ \varrho_1, \cdots, \varrho_t,\ \sigma_1, \cdots, \sigma_u$ are $r+s+t+u$ coprime matric variables. Then obviously h

and fg have the same absolute parity. The *product of the relative parities of* f, g is now defined to be the relative parity of h. Indicating this multiplication by juxtaposition we write

$$p(\lambda_1, \cdots, \lambda_r \ \mu_1, \cdots, \mu_s)\ p(\varrho_1, \cdots, \varrho_t \ \sigma_1, \cdots, \sigma_u)$$
$$\equiv p(\lambda_1, \cdots, \lambda_r, \ \varrho_1, \cdots, \varrho_t \mid \mu_1, \cdots, \mu_s, \ \sigma_1, \cdots, \sigma_u).$$

valid for any $r+s+t+u$ coprime matric variables $\lambda_l, \mu_m, \varrho_i, \sigma_j$. The arrangement of the matric variables within a symbol p being immaterial provided only that the bar be not crossed, it follows that *multiplication of relative parities is associative and commutative.* This multiplication has neither unity nor inverse. It is clear however that *with respect to multiplication the set of all coprime relative parities formed from a given set of matric variables is a semigroup.*

The notation being as above we have the following important special cases,

$$\prod_{i=1}^{r} p(\lambda_i \mid) = p(\lambda_1, \cdots, \lambda_r \mid), \quad \prod_{j=1}^{s} p(\mid \mu_j) = p(\mid \mu_1, \cdots, \mu_s),$$

$$\prod_{i=1}^{r} p(\lambda_i \mid) \prod_{j=1}^{s} p(\mid \mu_j) = p(\lambda_1, \cdots, \lambda_r \mid \mu_1, \cdots, \mu_s).$$

In the less obvious theory of addition of relative parities constructed next, the following remarks will be frequently assumed further notice. Let $\mu = \mu_a + \mu_b + \cdots + \mu_c$, be any partition of the matric variable μ, and let $\mu_e \equiv e_a\mu_a + e_b\mu_b + \cdots + e_c\mu_c$, where each e_j $(j = a, b, \cdots, c)$ is a definite one of $1, -1$, be any conjugate of this partition. Then $f(\mu \mid)$, $f(\mu_e \mid)$ have the same absolute parity $p(m \mid 0)$, where m is the order of μ, and similarly for $f(\mid \mu)$, $f(\mid \mu_e)$ and $p(0 \mid m)$. When μ is replaced by $-\mu$, μ_e becomes $-\mu_e$, and hence the true equations

$$f(-e_a\mu_a - \cdots - e_c\mu_c \mid) \equiv f(e_a\mu_a + \cdots + e_c\mu_c \mid),$$
$$f(\mid -e_a\mu_a - \cdots - e_c\mu_c) \equiv -f(\mid e_a\mu_a + \cdots + e_c\mu_c)$$

are implied by the single change of μ into $-\mu$. Again, illustrating for the simple case $\mu \equiv \mu_a + \mu_b$, we see that

$$f(\mu\,|),\quad f(\mu_a,\ \mu_b\,|)-f(|\,\mu_a,\ \mu_b)$$

have the same relative parity $p(\mu\ )$. For, if μ be changed to $-\mu$, $f(\mu\ )$ is unchanged in value, and under this change the difference becomes

$$f(-\mu_a,\ -\mu_b\,|)-f(|\,-\mu_a,\ -\mu_b),\ =\ f(\mu_a,\ \mu_b\,|)-f(|\,\mu_a,\ \mu_b).$$

Similarly for

$$f(|\,\mu),\ f(\mu_a\,|\,\mu_b)+f(\mu_b\,|\,\mu_a),$$

which have the same relative parity $p(|\,\mu)$, since

$$f(-\mu_a\,|\,-\mu_b)+f(-\mu_b\,|\,-\mu_a)\ =\ -f(\mu_a\,|\,\mu_b)-f(\mu_b\,|\,\mu_a).$$

As another illustration, let $\lambda = \lambda_a+\lambda_b-\lambda_c$, where λ_a, λ_b, λ_c are coprime matric variables. Then $f(|\,\lambda)$ and

$$f_1(\lambda_b,\ \lambda_c\,|\,\lambda_a)+f_2(\lambda_c,\ \lambda_a\,|\,\lambda_b)-f_3(\lambda_a,\ \lambda_b\,|\,\lambda_c)+f_4(|\,\lambda_a,\ \lambda_b,\ \lambda_c),$$

where f, $f_j\,(j = 1, \cdots, 4)$ are arbitrary beyond their indicated parities, have the same parity $p(|\,\lambda)$.

ABSTRACT IDENTITY OF $\mathfrak{P}$ WITH THE ALGEBRA $\mathfrak{T}$ OF THE CIRCULAR FUNCTIONS, §§ 7–9

7. The functions $\varphi_j\,(j = 0,1)$. Let $u, v, u_i, v_i\,(i = 1, 2, \cdots)$ be elements of a module $\mathfrak{M}$ in $\mathfrak{A}$, and let $\varphi_j(u)$ $(j = 0,1)$ be functions forming a ring $\mathfrak{R}_\varphi$ as u runs through all elements of $\mathfrak{M}$. Then, the indicated additions, multiplications, subtractions being operations of $\mathfrak{R}_\varphi$,

$$\begin{array}{lll} \varphi_0(u)\pm\varphi_1(v), & \varphi_0(u)\pm\varphi_0(v), & \varphi_1(u)\pm\varphi_1(v), \\ \varphi_0(u)\,\varphi_1(v), & \varphi_0(u)\,\varphi_0(v), & \varphi_1(u)\,\varphi_1(v) \end{array}$$

are in $\mathfrak{R}_\varphi$. The additions, subtractions in $\varphi_j(\pm u)$, $\varphi_j\ (u\pm v)$ $(j = 0,1)$ being now in $\mathfrak{M}$, these φ_j are in $\mathfrak{R}_\varphi$. On the set of all φ_j we henceforth impose the postulates

$$(7.1)\qquad \varphi_j(-u) = (-1)^j\varphi_j(u) \qquad (j = 0,1),$$

$$(7.2)\qquad \varphi_{1-j}(u+v) = \varphi_{1-j}(u)\,\varphi_0(v)+(-1)^j\varphi_j(u)\,\varphi_1(v)\ (j = 0,1).$$

From these follow, for $j = 0,1$ in each instance,

$$(7.3)\quad \varphi_{1-j}(u-v) = \varphi_{1-j}(u)\varphi_0(v) - (-1)^j \varphi_j(u)\varphi_1(v),$$

and therefore by (7.2)

$$(7.4)\quad 2\varphi_{1-j}(u)\varphi_0(v) = \varphi_{1-j}(u+v) + \varphi_{1-j}(u-v),$$

$$(7.5)\quad 2(-1)^j \varphi_j(u)\varphi_1(v) = \varphi_{1-j}(u+v) - \varphi_{1-j}(u-v).$$

In the instance $\mathfrak{F}_c$ of $\mathfrak{A}$ we define $\mathfrak{T}$ to be that part of trigonometry which, when $\varphi_0(u)$, $\varphi_1(u)$ are replaced by cos u, sin u respectively, is implied by (7.1), (7.2) *alone. When $\mathfrak{A}$ is abstract,* as always unless otherwise specified, *the set of all propositions implied by* (7.1), (7.2) *will be designed by $\mathfrak{R}_\varphi$.*

8. The $\mathfrak{P}$ isomorph of $\mathfrak{R}_\varphi$. We now solve (7.1)-(7.5) in terms of relative parity. Replace $u, v, u_i, v_i (i = 1, 2, \cdots)$ by a set $\lambda, \mu, \lambda_i, \mu_i (i = 1, 2, \cdots)$ of coprime matric variables. We recall that multiplication of relative parities was defined in § 6. Let ν be an arbitrary matric variable. Then

$$(8.1)\quad \varphi_0(\nu) \equiv p(\nu\,|), \quad \varphi_1(\nu) \equiv p(|\,\nu)$$

is a solution in this instance of (7.1). Under the substitutions (8.1) we get from (7.2)

$$(8.2)\quad p(\lambda+\mu\,|) = p(\lambda\,|)\,p(\mu\,|) - p(\,|\,\lambda)\,p(|\,\mu).$$

$$(8.3)\quad p(|\,\lambda+\mu) = p(|\,\lambda)\,p(\mu\,|) + p(\lambda\,|)\,p(\mu\,|),$$

or, what is the same by § 6,

$$(8.21)\quad p(\lambda+\mu\,|) = p(\lambda,\mu\,|) - p(|\,\lambda,\mu),$$

$$(8.31)\quad p(|\,\lambda+\mu) = p(\mu\,|\,\lambda) + p(\lambda\,|\,\mu),$$

which as yet are without significance. If a consistent interpretation can be assigned to (8.21), (8.31), we shall call (8.1) a $\mathfrak{P}$ *isomorph of* $\mathfrak{R}_\varphi$.

The interpretation to which we shall adhere is as follows. For (8.21): *an arbitrary $f(\lambda+\mu\,|)$ has the same relative parity $p(\lambda+\mu\,|)$ as the difference $f_1(\lambda,\mu\,|) - f_2(\,|\,\lambda,\mu)$, where f_1, f_2*

are arbitrary beyond the indicated relative parities $p(\lambda, \mu\,|)$, $p(\,|\,\lambda, \mu)$, *and similarly, mutatis mutandis, for* (8.31). Further, *we shall write these interpretations in the symbolic forms*

$$f(\lambda+\mu\,|) = f(\lambda, \mu\,|) - f(\,|\,\lambda, \mu), \tag{8.22}$$

$$f(\,|\,\lambda+\mu) = f(\lambda\,|\,\mu) + f(\mu\,|\,\lambda), \tag{8.32}$$

obtained by replacing p by f. Similarly, from (7.4) we write down (omitting the intermediate p forms)

$$2f(\lambda, \mu\,|) = f(\lambda+\mu\,|) + f(\lambda-\mu\,|), \tag{8.41}$$

$$2f(\lambda\,|\,\mu) = f(\,|\,\lambda+\mu) - f(\,|\,\lambda-\mu), \tag{8.42}$$

and from (7.5),

$$-2f(\,|\,\lambda, \mu) = f(\lambda+\mu\,|) - f(\lambda-\mu\,|), \tag{8.51}$$

whose interpretations are inverse to those of (8.22), (8.32) *in the following sense.* Note first that on the left of (8.22), (8.32) each function is of degree 1 (since $\lambda+\mu$ is a single matric variable in each case, thus $f(\lambda+\mu\,|)$ has the absolute parity $p(n\ 0)$, where n = the sum of the orders of λ, μ), while on the right each f is of degree 2; in (8.41)–(8.51) the exact reverse obtains. It will be sufficient now to interpret any one of (8.41)–(8.51), say the first. The constant multiplier 2 does not affect the parity of $f(\lambda, \mu\,|)$. *The interpretation of* (8.41) *is that* $f(\lambda, \mu\,|)$ (*or* $2f(\lambda, \mu\,|)$) *has the same relative parity* $p(\lambda, \mu\,|)$ *as the sum* $f_1(\lambda+\mu\,|) + f_1(\lambda-\mu\,|)$, *where* f, f_1 *are arbitrary. Note that in the interpretations of* (8.22)–(8.32) *the f's on the right typify different functions having the indicated parities, while in* (8.41)–(8.51) *they refer to the same function.*

To illustrate one of the important identical transformations discussed generally in a moment, apply (8.41), (8.51) to the right of (8.22). Then

$$f(\lambda+\mu\,|) = \frac{1}{2}[f(\lambda+\mu\,|) + f(\lambda-\mu\,|)] + \frac{1}{2}[f(\lambda+\mu\,|) - f(\lambda-\mu\,|)],$$

which in addition to checking the formal accuracy of the algebra gives us the following: an arbitrary function $f(\lambda+\mu)$ having the absolute parity $p(l+m\ 0)$, where l, m are the respective orders of λ, μ, is the sum of two functions of the respective absolute parities $p(l, m\ 0)$, $p(0\ l, m)$. This is the immediate consequence of applying to the processes yielding the above algebraic identity the appropriate interpretation as defined. After this detailed example there will be no dificulty in following the abstract discussion of the general case.

9. **Abstract identity of $\mathfrak{T}$, $\mathfrak{R}_\varphi$, $\mathfrak{P}$.** Let R be any relation in $\mathfrak{R}_\varphi$ of § 7 which is implied by (7.1), (7.2), and let R become T in the instance $\mathfrak{T}$ of $\mathfrak{R}_\varphi$. Suppose that interpretations can be assigned to the elements of $\mathfrak{A}$, giving an instance $\mathfrak{A}'$, such that (7.1), (7.2) are consistent in the instances $\mathfrak{M}'$, $\mathfrak{R}'_\varphi$ of $\mathfrak{M}$, $\mathfrak{R}_\varphi$ furnished by $\mathfrak{A}'$, and let R when interpreted in $\mathfrak{R}'_\varphi$ be R'. Then R' is implied by either of R, T, and hence all the true propositions in $\mathfrak{R}'_\varphi$, $\mathfrak{R}_\varphi$ can be written down from those in $\mathfrak{T}$.

We define $\mathfrak{P}$ *to be the set of all propositions implied by* (8.1)–(8.51), *or what is the same by* (8.21)–(8.51), *together with their interpretations as given in* § 8.

As is well known, $\mathfrak{T}$ is sufficient in $\mathfrak{F}_c$ for the deduction of De Moivre's theorem for a positive integral exponent, the expansion formulas expressing the sine or cosine of the sum of n arguments as a sum of products of sines and cosines of single arguments, and the decomposition of such products into sums or differences of sines or cosines of linear homogeneous functions of the arguments. It is precisely the abstractly identical equivalents in $\mathfrak{P}$ of these $\mathfrak{T}$ formulas that are important for applications. We shall write them down for $\mathfrak{R}_\varphi$ directly from $\mathfrak{T}$ by means of § 8 and the abstract identity noted above and then, by an application of $\mathfrak{P}$, infer immediately their interpretations for functions of matric variables having parity. What follows is more than a set of existence theorems; it gives a short way of obtaining the actual representations proved to exist in the $\mathfrak{P}$ theorems.

EXPANSION AND DECOMPOSITION IN $\mathfrak{P}$, §§ 10–14

10. Decomposition in $\mathfrak{R}_q$. For brevity we shall write

$$\varphi_j(u_1)\,\varphi_j(u_2)\cdots\varphi_j(u_r) \equiv \varphi_j(u_1, u_2, \cdots, u_r) \quad (j = 0, 1);$$

the indicated multiplications are in $\mathfrak{R}_q$. For either value of j this defines a species of multiplication, not necessarily that of $\mathfrak{R}_q$, under which the set of all $\varphi_j(u_1, \cdots, u_r)$ $(r = 1, 2, \cdots)$, as the u_i run through all elements of $\mathfrak{M}$, form a commutative semigroup according to

$$\varphi_j(u_1, \cdots, u_r)\,\varphi_j(v_1, \cdots, v_s) = \varphi_j(u_1, \cdots, u_r, v_1, \cdots, v_s) \quad (j = 0, 1).$$

On this multiplication we impose the postulate

$$\varphi_{1-j}(u_1, \cdots, u_r)\,\varphi_j(v_1, \cdots, v_s) = \varphi_j(v_1, \cdots, v_s)\,\varphi_{1-j}(u_1, \cdots, u_r) \quad (j = 0, 1),$$

so that with respect to it the $\varphi_j(u_1, \cdots, u_r)$ $(r = 1, 2, \cdots;$ $j = 0, 1)$ form a commutative semigroup. Since $\mathfrak{R}_q$ is a ring, this multiplication is distributive, as in $\mathfrak{A}$.

Let r, s be integers > 0, and let $\sum$ refer to all sets of values of the e_j each $= 1$ or -1. Then for $j = 1$ the generalizations, implied by $\mathfrak{T}$, of (7.4) in $\mathfrak{R}_q$ to r arguments is

$$(10.1)\quad 2^{r-1}\varphi_0(u_1, u_2, \cdots, u_r) = \sum \varphi_0(u_1 + e_2 u_2 + \cdots + e_r u_r),$$

and that of (7.5) to $2s$ arguments for $j = 1$ is

$$(10.2)\quad 2^{2s-1}(-1)^s \varphi_1(u_1, u_2, \cdots, u_{2s}) = \sum e_2 e_3 \cdots e_{2s}\,\varphi_0(u_1 + e_2 u_2 + \cdots + e_{2s} u_{2s}),$$

which is equivalent to

$$(10.21)\quad 2^{2s}(-1)^s \varphi_1(u_1, u_2, \cdots, u_{2s}) = \sum e_1 e_2 \cdots e_{2s}\,\varphi_0(e_1 u_1 + e_2 u_2 + \cdots + e_{2s} u_{2s});$$

also, when $t > 1$,

$$(10.3)\quad 2^{2t-2}(-1)^{t-1}\varphi_1(u_1, u_2, \cdots, u_{2t-1}) = \sum e_2 e_3 \cdots e_{2t-1}\,\varphi_1(u_1 + e_2 u_2 + \cdots + e_{2t-1} u_{2t-1}),$$

and if $t > 0$

$$(10.4)\quad 2^{2t-1}(-1)^{t-1}\varphi_1(u_1, u_2, \cdots, u_{2t-1}) = \sum e_1 e_2 \cdots e_{2t-1}\varphi_1(e_1 u_1 + e_2 u_2 + \cdots e_{2t-1}u_{2t-1}).$$

Each function on the left is a product in $\mathfrak{R}_\varphi$, thus $\varphi_0(u_1, \cdots, u_r) \equiv \varphi_0(u_1)\cdots\varphi_0(u_r)$, etc., while each right hand member is a linear homogeneous function in $\mathfrak{R}_\varphi$, with coefficients ± 1, of φ_0 or φ_1 functions, each of a single argument in $\mathfrak{M}$, the functions in a given instance being all φ_0 or all φ_1 according as the number of φ_1 factors in the $\mathfrak{R}_\varphi$ products on the left is even or odd. The number of terms on the right of (10.1)–(10.4) are respectively 2^{r-1}, 2^{2s-1}, 2^{2t-2}, 2^{2t-1}, a remark which will be assumed in writing down in § 15 the general $\mathfrak{P}$ theorem mentioned in § 5.

Either directly from the isomorphism with $\mathfrak{T}$ or from (10.1)–(10.4) we have the following generalizations of (7.4), (7.5) with $j = 0$, valid for integers r, s, $t > 0$,

$$(10.5)\quad 2^{r+2s-1}(-1)^s\varphi_0(u_1, u_2, \cdots, u_r)\varphi_1(v_1, v_2, \cdots, v_{2s}) = \sum \varepsilon_1\varepsilon_2\cdots\varepsilon_{2s}\varphi_0(u_1 + e_2 u_2 + \cdots + e_r u_r + \varepsilon_1 v_1 + \varepsilon_2 v_2 + \cdots + \varepsilon_{2s} v_{2s}),$$

where $\sum$ refers to all sets ef values of the e_i, ε_j ($i = 2, \cdots, r$; $j = 1, \cdots, 2s$), each $= \pm 1$;

$$(10.6)\quad 2^{r+2t-2}(-1)^{t-1}\varphi_0(u_1, u_2, \cdots, u_r)\varphi_1(v_1, v_2, \cdots, v_{2t-1}) = \sum \varepsilon_1\varepsilon_2\cdots\varepsilon_{2t-1}\varphi_1(u_1 + e_2 u_2 + \cdots + e_r u_r + \varepsilon_1 v_1 + \varepsilon_2 v_2 \cdots + \varepsilon_{2t-1} v_{2t-1}).$$

These contain respectively 2^{r+2s-1}, 2^{r+2t-2} terms. We shall refer to (10.1)–(10.6) as the *decomposition formulas* in $\mathfrak{R}_\varphi$.

11. **Expansion in $\mathfrak{R}_\varphi$.** The presence of $i = (-1)^{1/2}$ in an $\mathfrak{R}_\varphi$ identity signifies only that the coefficients of i, 1 are severally equal, precisely as in $\mathfrak{F}_c$, when the whole identity is reduced modulo $i^2 + 1$. De Moivre's theorem in $\mathfrak{T}$ is then abstractly identical in $\mathfrak{R}$ to

$$(11.1)\qquad \prod_{j=1}^{r}[\varphi_0(u_j)+i\,\varphi_1(u_j)] = \varphi_0\Big(\sum_{j=1}^{r}u_j\Big)+i\,\varphi_1\Big(\sum_{j=1}^{r}u_j\Big)$$

Comparing coefficients of 1, i in the distributed form of (11.1) we get the following *expansion formulas in* $\mathfrak{R}_f$,

$$(11.2)\qquad \varphi_0(u_1+u_2+\cdots+u_r) = A_r-\sum_2 A_{r-2}B_2+\sum_4 A_{r-4}B_4-\sum_6 A_{r-6}B_6+\cdots,$$

$$(11.3)\qquad \varphi_1(u_1+u_2+\cdots+u_r) = \sum_1 A_{r-1}B_1-\sum_3 A_{r-3}B_3+\sum_5 A_{r-5}B_5-\cdots,$$

in which $A_{r-j}B_j$ is the product of $r-j$ functions φ_0, each with only one of u_k $(k=1,\cdots,r)$ as argument, all the arguments being different, by j functions φ_1 whose arguments are the remaining u_k, and $\sum_j A_{r-j}B_j$ is the sum of all such products for j constant.

12. **The identical transformations I_ε, I_δ in $\mathfrak{R}_f$.** To each term on the right of (10.1) (10.6) apply the appropriate one of (11.2), (11.3) to expand. Then, directly from the abstract identity with $\mathfrak{T}$, it follows that the new right hand member reduces in each instance identically to the left. This process of expanding the decomposition of a function in $\mathfrak{R}_f$ will be called the *identical transformation* I_ε. If conversely (10.1) (10.6) be applied to decompose each product on the right of (11.2), (11.3), we get the *identical transformation* I_δ. These are fundamental in $\mathfrak{P}$.

13. **Expansion in $\mathfrak{P}$.** From the abstract identity of $\mathfrak{R}_f$, $\mathfrak{P}$ in § 9, and from the interpretation in § 8 of (8.22), (8.32), we can now infer the *general expansion formulas in* $\mathfrak{P}$, of which (8.22), (8.32) are the simplest instances, and infer immediately their interpretations. These and the like for decomposition can readily be verified independently by mathematical induction if desired, but this is superfluous.

In abstract identity with (11.2), (11.3) we now have

$$(13.1)\qquad f(\lambda_1+\lambda_2+\cdots+\lambda_r\,|\,) = A_r-\sum_2 A_{r-2}B_2+\cdots,$$

$$(13.2)\qquad f(\,|\,\lambda_1+\lambda_2+\cdots+\lambda_r) = \sum_1 A_{r-1}B_1-\sum_3 A_{r-3}B_3+\cdots.$$

in which λ_i $(i = 1, \cdots, r)$ is a set of coprime matric variables, and where now $A_{r-j}B_j$ denotes a function f having the relative parity indicated in

$$f(\mu_1, \mu_2, \cdots, \mu_{r-j} \mid \nu_1, \nu_2 \cdots, \nu_j),$$

where $\mu_k (k = 1, \cdots, r-j)$ is any set of $r-j$ matrices chosen from the set $\lambda_i (i = 1, \cdots, r)$, and $\nu_s (s = 1, \cdots, j)$ are the remaining j matrices in the λ_i set, and $\sum_j$, for j constant, refers to the sum of all such f's for the $r!/j!(r-j)!$ possible choices of the μ_k, ν_s. The interpretation is that *if the f's on the right are replaced by arbitrary $f_1, f_2, \cdots$ having the indicated relative parities, then the arbitrary f on the left has the same relative parity as the sum on the right, which is $p(A)$ in* (13.1), $p(\mid A)$ *in* (13.2) *where,* $A = \lambda_1 + \lambda_2 + \cdots + \lambda_r$.

14. **Decomposition in $\mathfrak{P}$.** From § 10 we infer, as in § 13, the decomposition formulas in $\mathfrak{P}$, where r, s, t are as in the correspondingly numbered formulas of § 10; the λ_i, $\mu_j (i = 1, 2, \cdots; j = 1, 2, \cdots)$ are coprime matric variables.

$$(14.1)\quad 2^{r-1} f(\lambda_1, \lambda_2, \cdots, \lambda_r) = \sum f(\lambda_1 + e_2\lambda_2 + \cdots + e_r\lambda_r),$$

$$(14.2)\quad 2^{2s-1}(-1)^s f(\mid \mu_1, \mu_2, \cdots, \mu_{2s}) = \sum e_2 e_3 \cdots e_{2s} f(\mu_1 + e_2\mu_2 + \cdots + e_{2s}\mu_{2s} \mid),$$

$$(14.3)\quad 2^{2t-2}(-1)^{t-1} f(\mid \mu_1, \mu_2, \cdots, \mu_{2t-1}) = \sum e_2 e_3 \cdots e_{2t-1} f(\mid \mu_1 + e_2\mu_2 + \cdots + e_{2t-1}\mu_{2t-1}),$$

$$(14.4)\quad 2^{2t-1}(-1)^{t-1} f(\mid \mu_1, \mu_2, \cdots, \mu_{2t-1}) = \sum e_1 e_2 \cdots e_{2t-1} f(\mid e_1\mu_1 + e_2\mu_2 + \cdots + e_{2t-1}\mu_{2t-1}),$$

$$(14.5)\quad 2^{r+2s-1}(-1)^s f(\lambda_1, \lambda_2, \cdots, \lambda_r \mid \mu_1, \mu_2, \cdots, \mu_{2s}) = \sum \varepsilon_1 \varepsilon_2 \cdots \varepsilon_{2s} f(\lambda_1 + e_2\lambda_2 + \cdots + e_r\lambda_r + \varepsilon_1\mu_1 + \varepsilon_2\mu_2 + \cdots + \varepsilon_{2s}\mu_{2s}),$$

$$(14.6)\quad 2^{r+2t-2}(-1)^{t-1} f(\lambda_1, \lambda_2, \cdots, \lambda_r \mid \mu_1, \mu_2, \cdots, \mu_{2t-1}) = \sum \varepsilon_1 \varepsilon_2 \cdots \varepsilon_{2t-1} f(\mid \lambda_1 + e_2\lambda_2 + \cdots + e_r\lambda_r + \varepsilon_1\mu_1 + \varepsilon_2\mu_2 + \cdots + \varepsilon_{2t-1}\mu_{2t-1}),$$

of which the interpretation is as follows: *if the several f's on the right of each of* (14.1) (14.6) *be replaced by the same*

f_1, arbitrary beyond the parity implied in the notation, then f on the left in each instance, arbitrary beyond the indicated parity, has the same relative parity as the sum on the right.

THE IDENTICAL TRANSFORMATIONS IN $\mathfrak{P}$, §§ 15-17

15. The general decomposition-expansion theorem in $\mathfrak{P}$. The following theorem is fundamental in the algebraic arithmetic of periodic functions. *If in*

$$f = f(\lambda_1, \cdots, \lambda_r \mid \mu_1, \cdots, \mu_s),$$

of absolute parity $p(a_1, \cdots, a_r \mid b_1, \cdots, b_s)$, the matric variables λ_i, μ_j be partitioned in any way into a'_j, b'_j new matric variables $(i = 1, \cdots, r;\ j = 1, \cdots, s)$, so that in the matric variables of all the partitions f has the absolute parity

$$p((a'_1, \cdots, a'_r \mid b'_1, \cdots, b'_s)),$$

and if

$$\omega' = \sum_{i=1}^{r} a'_i + \sum_{j=1}^{s} b'_j, \qquad \delta' = r + s, \qquad \omega' - \delta' = \varrho,$$

then f is a linear homogeneous function with coefficients ± 1 of 2^ϱ properly chosen functions of all the matric variables in the partitions, and the absolute parity of each of the 2^ϱ functions in the matric variables of the partitions is of the form $p((1^a\ 1^b))$, where $a + b = \omega'$.

When $a'_i = a_i$, $b'_j = b_j$ $(i = 1, \cdots, r;\ j = 1, \cdots, s)$, this degenerates to (5.2). The general theorem is the interpretation in $\mathfrak{P}$ of I_ε, I_δ. As a practicable method of obtaining the actual linear homogeneous function described is necessary in the algebraic arithmetic of periodic functions, we devise such a method next, and this implicitly contains a fuller proof of the theorem.

16. The identical algorithm in $\mathfrak{P}$. We saw that $\mathfrak{R}_q$, $\mathfrak{T}$, $\mathfrak{P}$ are abstractly identical. Hence we may operate in any one and interpret the results in each of the others. We shall operate in the familiar $\mathfrak{T}$ and infer $\mathfrak{P}$. As in the principle of duality in geometry a correspondence is established between

the elements and operations of the two systems which makes computations necessary in only one.

When interpreted in $\mathfrak{T}$ the Greek letters shall designate independent variables in $\mathfrak{F}_c$. when read in $\mathfrak{P}$ they shall denote coprime matric variables of any orders whose elements are in $\mathfrak{A}$. Sums and differences of variables in $\mathfrak{T}$. occurring as arguments. are as in $\mathfrak{F}_c$; in $\mathfrak{P}$ they are conjoints. and all differences indicate conjugates of partitions of matric variables. To

(16.1) $$f(\lambda_1, \cdots, \lambda_r | \mu_1, \cdots, \mu_s)$$

in $\mathfrak{P}$ corresponds

(16.12) $$\cos \lambda_1 \cdots \cos \lambda_r \sin \mu_1 \cdots \sin \mu_s$$

in $\mathfrak{T}$. and to

(16.21) $$f(\lambda_1 \pm \lambda_2 \pm \cdots \pm \lambda_r|), \quad f(|\mu_1 \pm \mu_2 \pm \cdots \pm \mu_s)$$

correspond respectively

(16.22) $$\cos(\lambda_1 \pm \lambda_2 \pm \cdots \pm \lambda_r), \quad \sin(\mu_1 \pm \mu_2 \pm \cdots \pm \mu_s).$$

Expansion in $\mathfrak{T}$ is merely the expression of (16.22) as sums of terms each of the type (16.12). for the appropriate r, s; decomposition is the reverse process of expressing (16.12) as sums (differences) of terms each of which is a cosine or sine of the form (16.22) according as s in (16.12) is even or odd. The transformations I_ε, I_δ in $\mathfrak{T}$ apply expansion (decomposition) to a function which has been derived in $\mathfrak{T}$ by decomposition (expansion). The correspondences (16.11)–(16.22) may be applied to $\mathfrak{P}$ by first obtaining I_ε. I_δ in $\mathfrak{T}$. translating to $\mathfrak{P}$. and then reading the results in accordance with §§ 13, 14. It is shorter and easier however to omit the intermediate $\mathfrak{T}$ formulas. All steps before the last are read as in $\mathfrak{T}$; in the final formulas we take the $\mathfrak{P}$ interpretation and get specific representations of functions having parity in the form demanded by § 15. We thus retain in the working of the algorithm all the advantages of familiarity with $\mathfrak{T}$ while dispensing with all superfluous intermediate identities. From the abstract identity of $\mathfrak{P}$, $\mathfrak{T}$ it follows that the systems of linear equations next introduced have always unique solutions.

The algorithm is reduced to the successive application of the two following. Note first that, the e_i, ε_j being positive or negative units as hitherto,

$$f(e_1\lambda_1, e_2\lambda_2, \cdots, e_r\lambda_r \mid \varepsilon_1\mu_1, \varepsilon_2\mu_2, \cdots, \varepsilon_s\mu_s)$$

has a unique *canonical form* $\pm f(\lambda_1, \cdots, \lambda_r \mid \mu_1, \cdots, \mu_s)$, where the sign is + or − according as the number of $\varepsilon_j (j = 1, \cdots, s)$ which are negative units is even or odd. To express $f(\lambda_1 + \lambda_2 + \cdots + \lambda_r)$ in the form demanded by § 15, we start from the descomposition (not from an expansion)

$$(16.3)\quad 2^{r-1} f(\lambda_1, \lambda_2, \cdots, \lambda_r) = \sum f(\lambda_1 + e_2\lambda_2 + \cdots + e_r\lambda_r).$$

Precisely one term on the right, that given by $e_i = 1$ $(i = 2, \cdots, r)$, is identical with the given f. Expand this term,

$$(16.4)\quad f(\lambda_1 + \lambda_2 + \cdots + \lambda_r) = A_r - \sum\nolimits_2 A_{r-2}\, B_2 + \cdots,$$

and from (16.4), by the appropriate changes of sign of the $\lambda_i (i = 2, \cdots, r)$, write down the expansions of the remaining $2^r - 2$ terms on the right of (16.3). Reduce all terms in these to canonical form. We now have a solvable set of 2^{r-1} linear equations for the 2^{r-1} functions f on the right of (16.4). The solution expresses each of these f's as a linear homogeneous function, with coefficients ± 1, of the 2^{r-1} functions $f(\lambda_1 + e_2\lambda_2 + \cdots + e_r\lambda_r)$, $e_i = \pm 1 (i = 2, \cdots, r)$. Each such expression has the same parity as the f from the right of (16.4) to which it is equated in the solution. Substituting the values thus obtained into (16.4) we have the expression of the left of (16.4) in the form demanded by § 15.

Similarly, to obtain the theorem in § 15 for $f(\mu_1 + \mu_2 + \cdots + \mu_s)$ we proceed in precisely the same way from the decomposition of $f(\mu_1, \mu_2, \cdots, \mu_s)$ if s is odd, while if s is even we may start from (among others, see (10.6)), $f(\mu_1, \mu_2, \cdots, \mu_{s-1}\ \mu_s)$.

Consider now the general case of (16.11), where some or all of $\lambda_i, \mu_j (i = 1, \cdots, r;\ j = 1, \cdots, s)$ are conjoints. Then regarding this f as a function of λ_i, say $f(\lambda_i\ *)$, and of μ_j,

say $f(* \mu_j)$ successively, and applying at each such step the preceding algorithm, we finally reach the actual representation required by § 15.

17. Example of § 16. To illustrate the algorithm we shall apply it to $f(\zeta|)$, $\zeta = \lambda + \mu + \nu$. Start from the decomposition

$$4f(\lambda, \mu, \nu|) = f(\lambda+\mu+\nu|)+f(\lambda+\mu-\nu|)+f(\lambda-\mu+\nu|)+f(\lambda-\mu-\nu|),$$

and write the typical expansion, (that of $f(\zeta)$) of a term on the right,

$$f(\lambda+\mu+\nu|) = f(\lambda, \mu, \nu|) - f(\lambda|\mu, \nu) - f(\mu|\nu, \lambda) - f(\nu|\lambda, \mu),$$

from which the expansions of the remaining three follow.

$$f(\lambda+\mu-\nu) = f(\lambda, \mu, \nu|) + f(\lambda|\mu, \nu) + f(\mu|\nu, \lambda) - f(\nu|\lambda, \mu).$$
$$f(\lambda-\mu+\nu) = f(\lambda, \mu, \nu) + f(\lambda|\mu, \nu) - f(\mu|\nu, \lambda) + f(\nu|\lambda, \mu),$$
$$f(\lambda-\mu-\nu) = f(\lambda, \mu, \nu) - f(\lambda|\mu, \nu) + f(\mu|\nu, \lambda) + f(\nu|\lambda, \mu).$$

The solution of the last 4 is

$$f(\lambda, \mu, \nu|) = \frac{1}{4}[\ f(\lambda+\mu+\nu|)+f(\lambda+\mu-\nu|)+f(\lambda-\mu+\nu|)+f(\lambda-\mu-\nu|)],$$

$$f(\lambda|\mu, \nu) = \frac{1}{4}[-f(\lambda+\mu+\nu|)+f(\lambda+\mu-\nu|)+f(\lambda-\mu+\nu|)-f(\lambda-\mu-\nu|)],$$

$$f(\mu|\nu, \lambda) = \frac{1}{4}[-f(\lambda+\mu+\nu|)+f(\lambda+\mu-\nu|)-f(\lambda-\mu+\nu|)+f(\lambda-\mu-\nu|)],$$

$$f(\nu|\lambda, \mu) = \frac{1}{4}[-f(\lambda+\mu+\nu|)-f(\lambda+\mu-\nu|)+f(\lambda-\mu+\nu|)+f(\lambda-\mu-\nu|)],$$

and it is evident that the sums on the right of these have the respective relative parities implied by the notations of the functions on the left. Substituting these into the expansion of $f(\xi)$, we have its expression as a linear homogeneous function of 4 functions having the respective absolute parities $p((1^3|0))$, $p((1\ 1^2))$, $p((1\ 1^2))$, $p((1\ 1^2))$ in the matric variables λ, μ, ν of the partition $\zeta = \lambda + \mu + \nu$ of ζ. This verifies § 15 in the case $\omega' = 3$, $\delta' = 1$, $\varrho = 2$.

DIVISIBILITY IN $\mathfrak{P}$, §§ 18–21

18. Divisibility of functions in general. We saw in § 6 that multiplication of relative parities generates a semi-

group in which there are no inverses. For the applications of $\mathfrak{P}$ to multiply periodic functions discussed in the next chapter it is necessary now to define a species of division for any class of functions φ which shall be abstractly identical, up to a certain point, with division in arithmetic. The consequences of the definition need be carried only so far as they relate to functions having parity, as no others enter algebraic arithmetic through periodic functions. The underlying structure in this type of division is abstractly that of class inclusion in mathematical logic or, if preferred, that of Dedekind's definition for divisibility of ideals. Inclusion here however appears with an additional restriction which has no abstractly identical equivalent in theories of the Dedekind or Kronecker types. It will be convenient to use the simplest notations of symbolic logic, thus $p \supset q$ for p implies q, $p :\equiv : q$ for $p \supset q \cdot q \supset p$, the dot between assertions signifying as usual the logical 'and'; also, irrespective of the precise meaning attached to *a divides b*, we shall write this as $a \mid b$, where the bar will not be confused with that which indicates parity.

Let $w_i = (x_i, y_i, \cdots, z_i)$ $(i = 1, \cdots, k)$ be any k values of the matric variable $w = (x, y, \cdots, z)$ of order n. Then, if there exist k constant scalars $c_i (i = 1, \cdots, k)$ not all zero such that

$$\sum_{i=1}^{k} c_i \varphi(w_i) = 0,$$

we shall say that *the function* $\varphi = \varphi(w)$ *vanishes over the matrix* ξ, *of* $n+1$ *columns and* k *rows,*

$$\xi = \begin{pmatrix} c_1 & x_1 & y_1 & \cdots & z_1 \\ c_2 & x_2 & y_2 & \cdots & z_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ c_k & x_k & y_k & \cdots & z_k \end{pmatrix}.$$

The extension to functions of $m > 1$ matric variables is obvious and need not be stated.

A Greek letter in square brackets, thus $[\xi]$, shall denote a set of matrices, and either of

$$[\xi]\varphi = 0, \qquad [\xi]\varphi(w) = 0,$$

shall signify that φ vanishes over each matrix in the set $[\xi]$, or as we shall say, φ *vanishes over* $[\xi]$. Each element of $[\xi]$ in the above has $n+1$ columns, but all do not necessarily have the same number of rows, nor do any two necessarily have a common element. If $\psi \equiv \psi(w)$ is any function of the matric variable w of order n we shall denote by $[\psi]$ the set of all matrices over which ψ vanishes, and call $[\psi]$ the *total set* of ψ. A total set may be null. Functions φ, ψ having the same total set are said to be *equal*, $\varphi = \psi$, and conversely, equality of functions is defined only in this sense.

The set σ (of any kind of elements) is said to *divide* (or *contain*) the set τ, $\sigma \mid \tau$, if each element of τ is in σ. A set therefore divides each of its elements. The *sum*, *product* of any number of sets are defined to be the logical sum, product respectively of all the sets, and *equality* of sets σ, τ is defined by

$$\sigma\ \tau \cdot \tau\ \sigma : __ : \sigma = \tau.$$

Let $\varphi \equiv \varphi(w)$, $\psi \equiv \psi(w)$ be functions of *the same matric variable w of order n*. Then the definition of divisibility for such functions is

(18.1) $$\varphi \mid \psi \ :\equiv: \ [\varphi]\psi = 0;$$

that is, φ *divides* (*or contains*) ψ *if and only if* ψ *vanishes over the total set of* φ. From the definitions we see at once the following,

(18.2) $$[\xi]\varphi = 0 \ :\equiv: \ [\varphi] \mid [\xi],$$

where $[\xi]$ is any set over which φ vanishes;

(18.3) $$\varphi \mid \psi \ :\equiv: \ [\psi] \mid [\varphi],$$

(18.4) $$\varphi \mid \psi \cdot \psi \mid \chi \ :\supset: \ \varphi \mid \chi,$$

(18.5) $$\varphi \mid \psi \cdot \psi \mid \varphi \ :\supset: \ \varphi = \psi,$$

and hence, from the last two, *division of functions is transitive and reflexive* as in arithmetic. We shall say that ψ in (18.1) is a *multiple* of φ. *Each multiple of φ vanishes over* $[\varphi]$.

19. Codivisors and comultiples of functions. A function φ which divides each of the functions $\psi, \cdots, \chi$ is called a *codivisor* of $\psi, \cdots, \chi$; if each of the functions $\psi, \cdots, \chi$ divides φ, φ is called a *comultiple* of $\psi, \cdots, \chi$. Similarly for sets. In what follows the logical sum, product of the total sets $[\varphi]$, $[\psi]$, $\cdots$, $[\chi]$ of the functions φ, $\psi, \cdots, \chi$ will be written $[\varphi + \psi + \cdots + \chi]$, $[\varphi\,\psi \cdots \chi]$.

Now $[\varphi\,\psi \cdots \chi]$ is the most inclusive set divisible by each of $[\varphi]$, $[\psi]$, $\cdots$, $[\chi]$, and $[\varphi + \psi + \cdots + \chi]$ is the least inclusive set which divides each of $[\varphi]$, $[\psi]$, $\cdots$, $[\chi]$. Hence each comultiple of $[\varphi]$, $[\psi]$, $\cdots$, $[\chi]$ is a multiple of $[\varphi\,\psi \cdots \chi]$, and each codivisor of $[\varphi]$, $[\psi]$, $\cdots$, $[\chi]$ divides also $[\varphi + \psi + \cdots + \chi]$. Moreover $[\varphi\,\psi \cdots \chi]$, $[\varphi + \psi + \cdots + \chi]$ are the only sets having these divisibility properties and hence, in abstract identity with rational arithmetic, we call them respectively the L. C. M. and the G. C. D. of $[\varphi]$, $[\psi]$, $\ldots$, $[\chi]$. We have

$$(19.1) \qquad [\psi]\,|\,[\varphi] \cdots [\chi]\,|\,[\varphi] \;:\equiv:\; [\psi \cdots \chi]\,|\,[\varphi];$$

that is, any comultiple $[\varphi]$ of $[\psi], \cdots, [\chi]$ is a multiple of their L. C. M. $[\psi \cdots \chi]$, and conversely, if $[\varphi]$ is a multiple of $[\psi \cdots \chi]$, then $[\varphi]$ is a multiple of each of $[\psi], \cdots, [\chi]$;

$$(19.2) \qquad [\varphi]\,|\,[\psi] \cdots [\varphi]\,|\,[\chi] \;:\equiv:\; [\varphi]\,|\,[\psi + \cdots + \chi],$$

which states that any codivisor $[\varphi]$ of $[\psi], \cdots, [\chi]$ divides their G. C. D. $[\psi + \cdots + \chi]$, and conversely, if $[\varphi]$ divides $[\psi + \cdots + \chi]$, then $[\varphi]$ divides each of $[\psi], \cdots, [\chi]$. Again,

$$[[\psi + \cdots + \chi]\;[\psi \cdots \chi]] = [\psi \cdots \chi],$$

by the law of absorption, and this asserts that the product of the G. C. D. and L. C. M. of the sets $[\psi], \cdots, [\chi]$ is equal to the product $[\psi \cdots \chi]$ of the sets.

The condition that the function φ shall be a codivisor of $\psi, \cdots, \chi$ is

$$(19.3) \qquad \varphi\,|\,\psi \cdots \varphi\,|\,\chi \;:\equiv:\; [\psi]\,|\,[\varphi] \cdots [\chi]\,|\,[\varphi];$$

and that φ shall be a comultiple of $\psi, \cdots, \chi$,

$$(19.4) \qquad \psi\,|\,\varphi \cdots \chi\,|\,\varphi \;:\equiv:\; [\varphi]\,|\,[\psi] \cdots [\varphi]\,|\,[\chi];$$

and hence, from (19.1)–(19.4),

$$(19.5) \qquad \varphi \mid \psi \cdots \varphi \mid \chi \;:\equiv:\; [\psi \cdots \chi] \mid [\varphi],$$

$$(19.6) \qquad \psi \mid \varphi \cdots \chi \mid \varphi \;:\equiv:\; [\varphi] \mid [\psi + \cdots + \chi];$$

that is, *if the function φ divides each of the functions $\psi, \cdots, \chi$, then the L. C. M. of the total sets of $\psi, \cdots, \chi$ divides the total set of φ, and conversely*; also, *if the function φ is a multiple of each of the functions $\psi, \cdots, \chi$, then the total set of φ divides the G. C. D. of the total sets of $\psi, \cdots, \chi$, and conversely.*

From (19.5), (18.3), (18.4) it now follows that

$$(19.7) \qquad \{\varphi \mid \psi \cdots \varphi \mid \chi\} \cdot \{[\psi \cdots \chi]\theta = 0\} \;:\supset:\; \varphi \mid \theta.$$

that is, *if each of $\psi, \cdots, \chi$ vanishes over the total set of φ, then so also does any function θ which vanishes over the total set $[\psi \cdots \chi]$ common to the total sets of $\psi, \cdots, \chi$.*

An example of θ such that $[\psi \cdots \chi]\theta = 0$ is $\theta =$ any linear homogeneous function of $\psi, \cdots, \chi$. The algebraic product of $\psi, \cdots, \chi$ does not in general vanish over $[\psi \cdots \chi]$.

From (19.5), (19.6) we now define the G. C. D. and L. C. M. of the functions $\psi, \cdots, \chi$. It is well to emphasize that these are sets, not functions. If in (19.5) we take $[\varphi] \equiv [\psi \cdots \chi]$, then

$$[\varphi]\varphi = 0 \;:\; -:\; [\psi \cdots \chi]\varphi = 0.$$

and φ is now any function vanishing over the L. C. M. of $[\psi], \cdots, [\chi]$. Since this choice gives the most inclusive $[\varphi]$ for which (19.5) holds we call φ *a greatest codivisor of $\psi, \cdots, \chi$ when* $[\varphi] \equiv [\psi \cdots \chi]$. Similarly, if in (19.6) we take $[\varphi]$ $[\psi + \cdots + \chi]$ we get the least $[\varphi]$ there possible, and any φ which vanishes over $[\psi + \cdots + \chi]$ is called *a least comultiple* of $\psi, \cdots, \chi$. Hence we take as the *unique* G. C. D., L. C. M. of a set of functions those *sets* whose elements are all the functions vanishing respectively over the L. C. M. and the G. C. D. of the total sets of the given functions.

By inverting the rôle of inclusion in the definition of divisibility for sets an alternative theory of division for functions, abstractly identical with the above, may be developed. In this, owing to the reciprocity between logical addition and multiplication, the parts played by addition and multiplication are inverted.

20. Application of division to $\mathfrak{P}$. When applied to $\mathfrak{P}$ the foregoing considerations have far reaching consequences, and it was to attain these, especially in the applications of $\mathfrak{P}$ to the algebraic arithmetic of periodic functions, that the divisibility of functions was devised. Before proceeding it will be well to notice the remarks at the end of § 6.

Let $\lambda = \mu + \nu + \cdots + \varrho$ be any partition of the matric variable λ. Then any function $F(\mu, \nu, \cdots, \varrho)$ (not necessarily possessing parity) is, with respect to simultaneous change of sign of all its matric variables $\mu, \nu, \cdots, \varrho$, a function of λ, for the change of λ into $-\lambda$ induces the change of $F(\mu, \nu, \cdots, \varrho)$ into $F(-\mu, -\nu, \cdots, -\varrho)$.

Suppose now that $f = f(\lambda\ )$, $g = g(\mid \lambda)$, λ as above, are entirely arbitrary beyond their indicated parities $p(\lambda\ )$, $p(\ \lambda)$, and let $F = F(\mu, \nu, \cdots, \varrho)$, $G = G(\mu, \nu, \cdots, \varrho)$ be any whatever functions having the respective parities $p(\lambda\ )$, $p(\mid \lambda)$ as just explained. Then

$$f \mid F, \qquad g \mid G; \tag{20.1}$$

for, f, g being arbitrary to the extent stated,

$$[f]f = 0 \,.\supset.\, [f]F = 0, \quad [g]g = 0 \,.\supset.\, [g]G = 0.$$

Thus, in our technical sense, F, G are multiples of f, g respectively.

Again, it is clear from (13.1), (13.2) that each term in the expansions there has the same parity $p(\lambda\ )$ or $p(\mid \lambda)$, where $\lambda = \lambda_1 + \lambda_2 + \cdots + \lambda_r$, as the functions expanded.

Hence if f, g are as in (20.1) *and F, G now denote any functions having any of the parities chosen as just indicated*

from the expansions of $f(\lambda\,|), f(\,|\lambda)$ *respectively, it follows that* (20.1) *holds for these* F, G *and therefore if* $f = 0$, $g = 0$ *over any set of matrices we infer immediately that* $F = 0$, $G = 0$ *over the same matrices. The relations* $[f]F = 0$, $[g]G = 0$ *are thus instances of* $[f]f = 0$, $[g]g = 0$ *respectively.*

According to our definitions F, G are multiples of f, g respectively. To illustrate the theorem we write out for a few simple functions their multiples obtained by expansion.

$\lambda =$	*Function*	*Multiples*
$\mu+\nu$	$f(\lambda\,\vert)$	$f(\mu, \nu\,\vert)$, $f(\vert\mu, \nu)$;
$\mu+\nu$	$f(\,\vert\,\lambda)$	$f(\mu\ \nu)$, $f(\nu\,\vert\,\mu)$;
$\mu+\nu+\varrho$	$f(\lambda\,\vert)$	$f(\mu, \nu, \varrho\,)$, $f(\mu\,\vert\,\nu, \varrho)$, $f(\nu\,\vert\,\mu, \varrho)$, $f(\varrho\,\vert\,\mu, \nu)$;
$\mu+\nu+\varrho$	$f(\vert\lambda)$	$f(\varrho, \mu\,\vert\,\nu)$, $f(\nu, \mu\,\vert\,\varrho)$, $f(\vert\mu, \nu, \varrho)$, $f(\nu, \varrho\,\vert\,\mu)$,

in all of which the f's are entirely arbitrary (and hence not connected by any relation) beyond the parities implied by their notations. Illustrating the last for example, we see that

$$\sum_i c_i\,(f(\vert\mu_i+\nu_i+\varrho_i) = 0$$

implies each of the following,

$$\sum_i c_i f(\vert\mu_i, \nu_i, \varrho_i) = 0, \qquad \sum_i c_i f(\nu_i, \varrho_i\vert\mu_i) = 0,$$
$$\sum_i c_i f(\varrho_i, \mu_i\vert\nu_i) = 0, \qquad \sum_i c_i f(\nu_i, \mu_i\vert\varrho_i) = 0.$$

Note that conversely *the last four together, but no fewer of them, imply the theorem from which they were inferred.* For, the f's being arbitrary to the extent stated, we may choose for them the approximate f's, having the same respective parities, as those occurring in the expansion of $f(\lambda+\mu+\nu)$ according to § 15. This remark is now generalized.

Let $\lambda = \mu+\nu+\cdots+\varrho$, *and let* $f_j(\mu, \nu, \cdots, \varrho)$ $(j = 1, 2, \cdots, k)$ *denote all the* f*'s occurring in the expansion of a definite one* $f(\lambda)$ *of* $f(\lambda\,\vert)$, $f(\vert\lambda)$. *Then*

$$(20.2) \qquad \sum_i c_i f_j(\mu_i, \nu_i, \cdots, \varrho_i) = 0 \qquad (j = 1, 2, \cdots, k)$$

together imply $\sum_i c_i f(\lambda_i) = 0$, *where* $\lambda_i = \mu_i + \nu_i + \cdots + \varrho_i$, *and no set of fewer than* k *of the relations* (20.2) *imply this conclusion.*

In all such theorems the complete arbitrariness of the functions except for their definite parities is to be noticed, as it is from this that their power and utility springs. We can now state a general theorem. *Regarding* $f \equiv f(\lambda, \mu, \cdots \cdots, \nu \mid \varrho, \sigma, \cdots, \tau)$ *as a function of each of the matric variables* $\lambda, \cdots, \tau$ *in turn, partitioning these in any way, and applying the theorem of § 15, we can write down from the vanishing of* f *over any matrix a system of equations for other* f*'s, arbitrary in the matric variables of the partitions, of relative parities in the partition variables given by the expansion of the original* f*; conversely, from all the latter equations, but from no fewer of them, we can infer the original.*

To illustrate, let $\lambda = \lambda_1 + \lambda_2$, $\mu = \mu_1 + \mu_2$. Then we have the following multiples of

$$f(\lambda \ \mu):$$

$$f(\lambda_1, \lambda_2 \mid \mu), \quad f(\mid \lambda_1, \lambda_2, \mu), \quad f(\lambda, \mu_1 \mid \mu_2), \quad f(\lambda, \mu_2 \ \mu_1),$$
$$f(\lambda_1, \lambda_2, \mu_1 \mid \mu_2), \quad f(\mu_1 \mid \lambda_1, \lambda_2, \mu_2),$$
$$f(\lambda_1, \lambda_2, \mu_2 \mid \mu_1), \quad f(\mu_2 \mid \lambda_1, \lambda_2, \mu_1),$$

giving in all 9 multiples of $f(\lambda \ \mu)$, itself included, in which each of λ, μ is partitioned into not more than 2 conjoints. The process can be continued so long as at least one λ_i, μ_j is of order > 1, and at any stage there are the possibilities of partitions of λ_i into l_i' conjoints, where $l_i' \leqq l_i$, $l_i =$ the order of λ_i, and similarly for μ_j. Finally, observing that any linear homogeneous function of any multiples of $f(\lambda \mid \mu)$ is a multiple of $f(\lambda \ \mu)$, we get further multiples, and the like applies to the general case. The complete generality of the multiples cannot be too strongly emphasized; the above theorems include all possible inferences concerning the vanishing over a given matrix to the vanishing of other

functions over the same matrix. It is necessary only that the parity of the functions be the same.

The general theorem can be given a slightly more general appearance by observing that in the *multiples* of a given $f(\lambda\,|)$ or $f(|\,\lambda)$, where $\lambda = \mu+\nu+\cdots+\varrho$, the $\mu, \nu, \cdots, \varrho$ may be replaced by $a\mu, b\nu, \cdots, c\varrho$, where $a, b, \cdots, c$ are scalars different from zero. This however is a special case of the theorem, and it illustrates the above remarks on the generality of the functions involved.

By successive applications of expansion and decomposition to the arbitrary f's of parity $p(a_1, \cdots, a_r\,|\,b_1, \cdots, b_s)$ in any sum of such f's vanishing over a given matrix we can *generate a closed set of vanishing sums for arbitrary functions having parity*. The number of such sums is an ordinary partition function of the a_i, b_j which depends upon the combinational function $\Pi(\omega)$ mentioned in § 26 of the preceding chapter.

21. Parity transformations. A transformation of the matric variables of a function f having parity which leaves invariant the absolute parity of f is called *parity transformation*; and the result of the transformation a *parity transform* of the original function. These play an important part in the deduction of special cases of the general theorems inferred from periodic functions in the next chapter. There seems to be no simple means of defining the most general parity transformation, but we note the following useful instances. Let $z \equiv (z_1, \cdots, z_n)$ be a matric variable of order n, and let $f_j(z\,|), g_j(|\,z)$ $(j = 1, \cdots, n)$ be arbitrary of the indicated parities. Define new matric variables Z_0, Z_1 of order n, by

$$Z_0 \equiv (f_1(z\,|), f_2(z\,|), \cdots, f_n(z\,|)),$$
$$Z_1 \equiv (g_1(|\,z), g_2(|\,z), \cdots, g_n(|\,z)).$$

Then each of $f(Z_0)$, $f(Z_0)$, $f(Z_1)$ is a parity transform of $f(z)$, and $f(Z_1)$ is a parity transform of $f(z)$. More generally, if the respective orders of the matric variables λ_i, μ_j be $a_i, b_j (i = 1, \cdots, r;\ j = 1, \cdots, s)$, a parity transform of $f(\lambda_1, \cdots, \lambda_r\,|\,\mu_1, \cdots, \mu_s)$ is given by replacing each

variable in λ_i by an arbitrary function of parity $p(a_i|0)$ or $p(0\ a_i)$ in all the variables of λ_i, and each variable in μ_j by an arbitrary function of parity $p(0\ b_j)$ in all the variables of $\mu_j (i = 1, \cdots, r;\ j = 1, \cdots, s)$.

From § 20 it is clear, that *if F is a parity transform of the arbitrary f having parity, then f F.*

ALGEBRAIC PARITY, GENERALIZATION OF $\mathfrak{P}$, § 22

22. Parity in an algebraic number field. The so-called functions with recurring derivatives of Olivier, Nicodemi, Glaisher, Appell and others suggest a wide generalization of the concept of parity as defined in § 2. The functions just mentioned are the simplest instances of certain functions in n variables with n periods related to an algebraic number field of degree n. The functions of Olivier and others refer to the very special case in which the field is generated by a primitive nth root of unity. In the general case the field is defined by any irreducible equation of degree n. There are associated with the field sets of n functions which are linearly dependent when the variables are multiplied by numbers in the field. The theory of parity as developed above refers to the simplest of all instances, namely that in which the equation defining the field is $x + 1 = 0$. As the generalization is extremely extensive, and as it leads to a new domain of algebra, we shall not pursue it further here, but may refer (for certain algebraic details) to a paper in the *Quarterly Journal* (1926-7) on *N-fold periodic functions connected with an algebraic number field of degree N.*

CHAPTER III

THE ALGEBRAIC ARITHMETIC OF MULTIPLY PERIODIC FUNCTIONS

THE PRINCIPLE OF PARAPHRASE, §§ 1–5

1. Application of parity to periodic functions. The algebra $\mathfrak{P}$ has immediate applications to the algebraic arithmetic of n-fold periodic functions, $n \geqq 1$. When $n = 1$ the application leads to the numbers, polynomials and functions of Bernoulli, Euler, Genocchi and Lucas in a rather unexpected way, also to the novel generalizations of all these implicit in the algebra of elliptic functions. This application is developed by means of $\mathfrak{B}$ and a subalgebra of the latter abstractly identical with $\mathfrak{T}$. But as the application of $\mathfrak{P}$ to the n-fold periodic functions when $n > 1$ leads to a far richer theory than that just indicated, we shall discuss the case $n > 1$ alone. Under n-fold periodic functions we include the pseudo-periodic, for example the doubly periodic functions of the rth kind, $r > 1$, of Hermite and others, and the theta functions of $p > 1$ arguments. Unless otherwise stated *theta* shall mean elliptic theta function, and *theta quotient* any rational function of theta functions. Hence in particular the elliptic functions and certain of the doubly periodic functions of the rth kind are theta quotients as here defined.

The n-fold periodic functions are connected with algebraic arithmetic through the circular functions in the following manner. Consider first the case $n = 2$. In the usual notation any theta quotient has a twofold type of expansion, first as a power series in q, the coefficient of the general power of q being a function of the exponent or of its divisors and circular functions of the arguments, second, as a Fourier series. The latter, upon expansion of the coefficients of the trigonometric terms into power series in q yields a series of

the first species, which we shall call an *arithmetical expansion*. In the above we have neglected temporarily terms involving reciprocals of sines or cosines; see § 13. Such expansions are not current in the literature because their principal interest is for the theory of numbers, especially for that branch of it in which we are at present interested. The arithmetical expansion of a theta quotient is unique (including the terms in reciprocals of sines or cosines). If in any identity between theta quotients the several terms be replaced by their arithmetical expansions, and if in the result coefficients of like general powers of q be compared, we get a trigonometric identity which, as will be shown, implies and is implied by an identity between arbitrary functions having parity. The identity between parity functions is therefore formally equivalent to the given theta identity; it presents all of the arithmetical information implicit in the theta identity in a concise, suggestive form, and conversely, from the parity identity that between theta quotients can be recovered by specialization of the parity functions to circular functions having the same respective absolute parities.

When $n = 1$ there are no arithmetical expansions as above defined. Hence the algebraic arithmetic of the singly periodic functions is radically different from that given by the case $n > 1$.

When $n > 2$ there enter, in place of the single parameter q several, say $r > 1$. With respect to these r parameters it can be shown that arithmetical expansions exist and that, proceeding from these in the same way as when $n = 2$, we should reach systems of not less than r arithmetical identities between arbitrary functions formally equivalent to a single identity between n-fold periodic functions. The r-fold generalization of $\mathfrak{C}$ mentioned in the first chapter appears naturally in this connection. But when $n > 2$, except in the case where no theta function occurs in the denominator, the arithmetical expansions have not been obtained, and it seems to be a matter of considerable difficulty to elicit from Appell's expansions ($n = 4$) forms appropriate for arithmetic. Were these

expansions completely known we could more than double the extant arithmetic of systems of quadratic and certain higher forms in any number of indeterminates at one step.

2. **Parity functions.** Thus far we have discussed functions having parity without distinguishing the instances according to those, $\mathfrak{A}_j$, of $\mathfrak{A}$, in which the matric variables lie. The expansion and decomposition theorems in $\mathfrak{P}$ require only that the matric variables be in a ring $\mathfrak{R}$ of $\mathfrak{A}$. Let $\mathfrak{R}_j$ be a ring in the instance $\mathfrak{A}_j$ of $\mathfrak{A}$, and let f be a function having parity. Then, if for each set of values in $\mathfrak{R}_j$ of all its matric variables f takes a single definite value in $\mathfrak{A}_j$, and if further f vanishes with each matric variable with respect to which f has an odd absolute parity, we shall call f a *parity function in* $\mathfrak{A}_j$ or, when $\mathfrak{A}_j$ is understood, a *parity function*. In general $\mathfrak{A}_j$ will be $\mathfrak{F}_r$, although a considerable part of the main theorem is proved in $\mathfrak{A}$. It is emphasized that *beyond the three restrictions stated, namely that f is uniform with respect to values of the matric variables in the ring concerned, f possesses parity, f vanishes with each matric variable occurring to the right of the bar in its symbol $f(*\,|\,\dot{+})$, the parity function f is completely arbitrary.* If the parity of f and its uniformity with respect to integral arguments be preserved, but further conditions be imposed upon f giving, say, F, we shall call F a *restricted parity function.*

3. **Principle of paraphrase, first form.** Let a_i, b_j $(i = 1, \cdots, r;\ j = 1, \cdots, s)$ denote δ integers > 0, and write

$$a_1 + \cdots + a_r \equiv \omega_0, \quad b_1 + \cdots + b_s \equiv \omega_1, \quad r \equiv \delta_0, \quad s \equiv \delta_1,$$
$$\omega \equiv \omega_0 + \omega_1, \quad \delta \equiv \delta_0 + \delta_1,$$

as in chapter II § 4. In what follows the x, y with suffixes in the δ matric variables ξ, η with suffixes are ω independent variables in $\mathfrak{F}_c$,

$$\xi_i \equiv (x_{i1}, x_{i2}, \cdots, x_{ia}) \quad (a \equiv a_i;\ i = 1, \cdots, r),$$
$$\eta_j \equiv (y_{j1}, y_{j2}, \cdots, y_{jb}) \quad (b \equiv b_j;\ j = 1, \cdots, s);$$

the u, v with suffixes in the following $n\delta$ matric variables with suffixes are $n\omega$ rational integers,

$$\alpha_{ik} \equiv (u_{i1k}, u_{i2k}, \cdots, u_{iak}) \quad (a \equiv a_i; \quad i = 1, \cdots, r),$$
$$\beta_{jk} \equiv (v_{j1k}, v_{j2k}, \cdots, v_{jbk}) \quad (b \equiv b_j; \quad j = 1, \cdots, s),$$
$$(k = 1, \cdots, n).$$

In writing functions $\varphi((\alpha\xi))$ of scalar products $(\alpha\xi)$ we shall omit one ( ) and write simply $\varphi(\alpha\xi)$. From the above matric variables form scalar products as follows,

$$(\alpha_{ik}\,\xi_i) \equiv u_{i1k}\,x_{i1} + u_{i2k}\,x_{i2} + \cdots + u_{iak}\,x_{ia},$$
$$(\beta_{jk}\,\eta_j) \equiv v_{j1k}\,y_{j1} + v_{j2k}\,y_{j2} + \cdots + v_{jbk}\,y_{jb},$$
$$(a \equiv a_i,\ b \equiv b_j;\ \ i = 1, \cdots, r;\ \ j = 1, \cdots, s;\ \ k = 1, \cdots, n).$$

Let each of the following f, g, h be a parity function in $\mathfrak{F}_r$, the ring $\mathfrak{R}_r$ in which the matric variables lie being that of the rational integers,

$$(3.01)\quad f(\xi_1, \cdots, \xi_r|\eta_1, \cdots, \eta_s),\quad g(\xi_1, \cdots, \xi_r|),\quad h(|\eta_1, \cdots, \eta_s),$$

of which the respective absolute parities are

$$(3.02)\quad p(a_1, \cdots, a_r|b_1, \cdots, b_s),\quad p(a_1, \cdots, a_r|0),\quad p(0|b_1, \cdots, b_s),$$

and the orders, degrees are respectively

$$\omega, \delta; \qquad \omega_0, \delta_0; \qquad \omega_1, \delta_1.$$

Let q_k, l_k, t_k $(k = 1, \cdots, n)$ be constant integers. The generalization of what follows to the case where the q_k, l_k, t_k are considered as elements of $\mathfrak{F}_c$ is not essential, as it can always be reduced to the simultaneous assertion of one or more theorems of the type stated.

We can now formulate the *principle of paraphrase*. *If a particular one of*

$$(3.11)\quad \sum_{k=1}^{n}\left\{q_k\left[\prod_{i=1}^{r}\cos(\alpha_{ik}\,\xi_i)\prod_{j=1}^{s}\sin(\beta_{jk}\,\eta_j)\right]\right\} = 0,$$

$$(3.21)\quad \sum_{k=1}^{n}\left\{l_k\left[\prod_{i=1}^{r}\cos(\alpha_{ik}\,\xi_i)\right]\right\} = 0,$$

$$(3.31)\quad \sum_{k=1}^{n}\left\{t_k\left[\prod_{j=1}^{r}\sin(\beta_{jk}\,\eta_j)\right]\right\} = 0,$$

is an identity in all of the x, y variables (with suffixes) occurring in the ξ_i, η_j present, then that one implies and is implied by the corresponding one of

$$(3.12)\quad \sum_{k=1}^{n} q_k f(\alpha_{1k}, \alpha_{2k}, \cdots, \alpha_{rk}, \beta_{1k}, \beta_{2k}, \cdots, \beta_{sk}) = 0,$$

$$(3.22)\quad \sum_{k=1}^{n} l_k g(\alpha_{1k}, \alpha_{2k}, \cdots, \alpha_{rk}) = 0,$$

$$(3.32)\quad \sum_{k=1}^{n} t_k h(\beta_{1k}, \beta_{2k}, \cdots, \beta_{sk}) = 0,$$

where f, g, h are as in (3.01).

The implication of (3.j1) by 3.j2 ($j = 1, 2, 3$) is evident since the trigonometric products are instances of f, g, h respectively. Again, (3.12), and hence (3.11) implies (3.32) but not (3.22). Hence it remains only to prove that (3.11) implies (3.12) and that (3.21) implies (3.22). The last two proofs will presently be reduced to that of the special case of (3.22) in which g is of parity $p(n \mid 0)$.

In the above statement the α, β matrices are in $\mathfrak{F}_r$. We shall prove much more than this. It will be shown that if *the α, β matrices are in $\mathfrak{A}$, and the circular functions also are in $\mathfrak{A}$, then* (3.21) *implies* (3.22), *and when $s = \delta_1$ in* (3.11). (3.31) *is even, these imply* (3.12), (3.32) *respectively in* $\mathfrak{A}$. The two excepted cases of this generalization from $\mathfrak{F}_r$ to $\mathfrak{A}$ when δ_1 is an odd integer also appear for several reasons to be true, but I am unable to prove them in $\mathfrak{A}$. The extensions to $\mathfrak{A}$ are however only of algebraic interest, as they can never occur in ordinary analysis or in any of its arithmetical consequences, for such analysis is based on either $\mathfrak{F}_c$ or $\mathfrak{F}_r$. In particular the algebraic extensions to $\mathfrak{A}$ are irrelevant for the arithmetic of periodic functions. Simple applications of the principle are given in §§ 14 16.

4. Second form of the principle. Before proceeding to the necessary proofs of § 3 we shall state and prove a *modified form* of the principle. This modification will cover most, but by no means all, of the applications of the parity identities that will ordinarily suggest themselves. What

follows differs from the first statement in this important respect: *it is further postulated that in some domain the parity functions have convergent power series expansions.* The *modified principle* applies therefore only to *restricted parity functions* (analytic), the principle in § 3 to *unrestricted* (not necessarily analytic) parity functions. For what follows I am indebted to Professor G. Y. Rainich; it has not been published elsewhere.

Let $F \equiv F(x_1, \cdots, x_n)$ be a function of n independent variables $x_1, \cdots, x_n$ in $\mathfrak{F}_c$ or $\mathfrak{F}_r$ which has a power series expansion

$$F = \sum A(i_1, \cdots, i_n)\, x_1^{i_1} \cdots x_n^{i_n} \tag{4.1}$$

converging in some domain Δ. In general some of the coefficients $A(i_1, \cdots, i_n)$ $(i_j = 0, 1, \cdots; j = 1, \cdots, n)$ will be zero. Let $G \equiv G(x_1, \cdots, x_n)$ also have an expansion

$$G \equiv \sum B(i_1, \cdots, i_n)\, x_1^{i_1} \cdots x_n^{i_n} \tag{4.2}$$

convergent in Δ. The coefficients $A \equiv A(i_1, \cdots, i_n)$, $B \equiv B(j_1, \cdots, j_n)$ of two terms in (4.1), (4.2) are said to *correspond* when and only when $(i_1, \cdots, i_n) = (j_1, \cdots, j_n)$ (matric equality), and G is said *not to exceed the type of* F when those coefficients B which correspond to zero coefficients A also vanish.

For example, no even analytic function exceeds the type of $\cos x$, since all those coefficients of a power series representing an even function which correspond to the vanishing coefficients (those of $x, x^3, x^5, \cdots$) in the expansion of $\cos x$ must vanish. Again, x^2 does not exceed the type of $\cos x$, but not conversely since the coefficient of x^4 in x^2 vanishes while the corresponding coefficient in $\cos x$ is 1/24.

Suppose now that for a given $F(x_1, \cdots, x_n)$ there exist $(n+1)m$ constants

$$c_1, \cdots, c_m;\ a_{j1}, \cdots, a_{jm} \qquad (j = 1, \cdots, n)$$

such that

$$\sum_{j=1}^{m} c_j F(a_{1j} x_1, \cdots, a_{nj} x_n) = 0 \tag{4.3}$$

is an identity in the $x_j\,(j = 1, \cdots, n)$. Then, *if a function F satisfies an identity* (4.3) *the same identity holds for every function G which does not exceed the type of F.*

To prove this, replace $F(x_1, \cdots, x_n)$ by its power series. The left of (4.3) takes the form of an identically vanishing power series. Hence each coefficient vanishes. But these coefficients are linear combinations of terms of the form

$$A(i_1, \cdots, i_n)\ a_{1j}^{i_1} \cdots a_{nj}^{i_n}, \tag{4.4}$$

namely,

$$\sum_{j=1}^{m} c_j A(i_1, \cdots, i_n)\ a_{1j}^{i_1} \cdots a_{nj}^{i_n}, \equiv A(i_1, \cdots, i_n) \sum_{j=1}^{m} c_j\, a_{1j}^{i_1} \cdots a_{nj}^{i_n}. \tag{4.5}$$

Since the last product vanishes, at least one of $A(i_1, \cdots, i_n)$, $\sum c_j\, a_{1j}^{i_1} \cdots a_{nj}^{i_n}$ must vanish for every set of values of $(i_1, \cdots, i_n)$. Consider now the expression corresponding to the left of (4.3) which is derived from a function $G(x_1, \cdots, x_n)$ which does not exceed the type of F. On substituting for G its power series expansion we get a power series whose coefficients are of the form

$$B(i_1, \cdots, i_n) \sum_{j=1}^{m} c_j\, a_{1j}^{i_1} \cdots a_{nj}^{i_n}. \tag{4.6}$$

Compare (4.5), (4.6), and recall that (4.5) vanishes in all cases. If for a particular value of $(i_1, \cdots, i_n)$, (4.5) vanishes on account of the $\sum$ factor vanishing, then (4.6) vanishes because its $\sum$ factor is identical with that of (4.5). If on the other hand (4.5) vanishes with $A(i_1, \cdots, i_n)$ for the particular value of $(i_1, \cdots, i_n)$, then $B(i_1, \cdots, i_n)$ vanishes for the same value, since G does not exceed the type of F. Hence in all cases (4.6) vanishes, and therefore

$$\sum_{j=1}^{m} c_j\, G(a_{1j}\, x_1, \cdots, a_{nj}\, x_n) \equiv 0, \tag{4.7}$$

which is the theorem.

To apply this to the *restricted principle*, consider an analytic f (— possessing a convergent power series expansion in all its variables) having parity $p(2\ 3)$. This will suffice, as the proof for f having any absolute parity is precisely similar; we start in any instance from the simplest circular function having the same parity. Consider then

$$(4.8) \quad f(x, y; u, v, w) \equiv \cos(x+y)\ \sin(u+v+w),$$

where x, y, u, v, w are independent variables in F_c. The sum of the exponents of x and y in each term of the expansion of (4.8) is even, the like sum for u, v, w is odd; the coefficient of any term violating these conditions is zero. Let $f = f((x, y)\ (u, v, w))$ be a restricted (as to analyticity) parity function having, as indicated, the same parity $p(2\ 3)$ as (4.8), which is defined for integral values of its arguments. We may now consider an analytic function which will assume the same values as f for integral values of the arguments.*

The latter function will not exceed the type of (4.8), and hence it will satisfy any identity of the form (4.3) which is satisfied by (4.8).

The following illustrations (due to Professor Rainich) throw further light on the nature of the restricted principle. An example of (4.3) with $n = 1$, $m = 2$ is $f(x)+f(-x) \equiv 0$, in which the coefficients c, a are $c_1 = c_2 = 1$, $a_1 = -a_2 = 1$. This is satisfied by every function which does not exceed the type of $\sin x$, namely, by every odd function.

Consider next

$$f(x+y) - f(x) - f(y) + f(0) \equiv 0.$$

Here $F(x, y) \equiv f(x+y)$, $n = 2$, $m = 4$, and the coefficients c, a are

$$c_1 = -c_2 = -c_3 = c_4 = 1,$$
$$a_1 = a_2 = 1, \qquad a_3 = a_4 = 0,$$
$$b_1 = b_3 = 1, \qquad b_2 = b_4 = 0.$$

* Appeal is made here to a well known theorem of Borel (proved by him, however, only for functions of one variable).

The identity is satisfied by any function which does not exceed the type of $1+x+y$, for example $A(x+y)+B$, where A, B are independent of x, y.

In the following example $n=1$, $m=3$. Take

$$\begin{vmatrix} f(ax) & f(bx) & f(cx) \\ a & b & c \\ 1 & 1 & 1 \end{vmatrix} \equiv 0,$$

as the instance of (4.3). Here

$$c_1 = b-c, \quad c_2 = c-a, \quad c_3 = a-b,$$
$$a_1 = a, \quad a_2 = b, \quad a_3 = c,$$

and the functions f are linear, $A+Bx$, or functions which do not exceed the type of $1+x$.

As a last example, consider functions illustrating the algebraic parity mentioned in § 22 of Chapter II. Let α be a complex cube root of unity, and write

$$f_j(x) \equiv \exp x + \alpha^j \exp \alpha x + \alpha^{2j} \exp \alpha^2 x \qquad (j = 0, 1, 2).$$

Then in the development of $f_j(x)$ only exponents $j \bmod 3$ appear. Consider now, for example, functions which do not exceed the type of

$$f_0(x+y) \quad f_0(u+v) \quad f_1(p+q+r) \quad f_2(s+t).$$

Their expressions will be characterized by the vanishing of certain coefficients, or by the property that if x, y are replaced by αx, αy, the function is unchanged in value, while if p, q, r are replaced by αp, αq, αr the function acquires the factor α, etc.

5. Algebraic lemmas. We return now to the principle as stated in § 3 and outline a purely algebraic proof. The following differs from the original proof given in the *Transactions*, vol. 22 (1921) p. 1, and it applies to more general situations. The algebraic lemmas themselves are not without interest.

A reference to any treatise on algebraic equations, or to MacMahon's *Combinatorial Analysis*, will show that Waring's (or Girard's) theorems on symmetric functions are mere identities in $\mathfrak{A}$, to prove which are required only the postulates of an abstract field and their immediate consequences; this is also evident from Kronecker's theory (see for example König, *Algebraische Größen*) of elimination. We shall therefore state and prove our lemmas for $\mathfrak{A}$, although the applications which we have in view refer to $\mathfrak{P}$ in $\mathfrak{F}_c$ or $\mathfrak{F}_r$.

Let c_i $(i = 1, \cdots, b)$, $\gamma_j (j = 1, \cdots, \beta)$ be sets of elements in $\mathfrak{A}$, and write

$$s_m \equiv c_1^m + c_2^m + \cdots + c_b^m, \quad \sigma_m \equiv \gamma_1^m + \gamma_2^m + \cdots + \gamma_\beta^m \quad (m = 0, 1, \cdots),$$

$(-1)^k p_k \equiv$ the kth elementary symmetric function $(k = 1, \cdots, b)$ of the c_i $(i = 1, \cdots, b)$, and $(-1)^l \pi_l \equiv$ the lth elementary symmetric function $(l = 1, \cdots, \beta)$ of the γ_j $(j = 1, \cdots, \beta)$; $p_0 = \pi_0 = 1 \equiv$ the unity in $\mathfrak{A}$. Without loss of generality assume $\beta \geq b$. We shall prove that

$$s_m = \sigma_m \qquad (m = 1, \cdots, \beta) \tag{5.1}$$

implies that $\beta - b$ *of the* γ_j $(j = 1, \cdots, \beta)$ *vanish, and that the remaining* b *of the* γ_j *are a permutation of the* c_i $(i = 1, \cdots, b)$.

Let the x_j be in $\mathfrak{A}$. With the usual convention $0! = 1$, and with $\sum$ referring to all sets of m integers r_t $(t = 1, \cdots, m)$ each ≥ 0 such that $r_1 + 2r_2 + 3r_3 + \cdots m r_m = m$, write

$$\varphi(x_1, x_2, \cdots, x_m) \equiv \sum [(c_m X_m)/(A_m B_m)],$$
$$c_m \equiv (-1)^{r_1 + r_2 + \cdots + r_m}, \qquad X_m \equiv x_1^{r_1} x_2^{r_2} \cdots x_m^{r_m},$$
$$A_m \equiv r_1! \, r_2! \cdots r_m!, \qquad B_m \equiv 1^{r_1} 2^{r_2} \cdots m^{r_m}.$$

In the instance $\mathfrak{F}_c$ of $\mathfrak{A}$, φ is a familiar expression occurring in connection with Waring's theorems. Write

$$\varphi(s_1, s_2, \cdots, s_m) \equiv P_m, \qquad \varphi(\sigma_1, \sigma_2, \cdots, \sigma_m) \equiv \Pi_m.$$

Then, by (5.1), we have in particular

$$P_r = \Pi_r \qquad (r = 1, \cdots, \beta). \tag{5.2}$$

Again, by a well known theorem on symmetric functions in $\mathfrak{F}_c$ which, as pointed out, goes over unchanged into $\mathfrak{A}$,

$$P_i = p_i\,(i = 1, \cdots, b),\ P_j = 0\,(j > b), \quad \Pi_k = \pi_k\,(k = 1, \cdots, \beta). \tag{5.3}$$

Hence the following is an identity in the (Kronecker) indeterminate w,

$$\sum_{i=0}^{\beta} \pi_i w^{\beta-i} \equiv \sum_{j=0}^{b} p_j w^{\beta-j} + \sum_{j=b}^{\beta-b} P_{b+j} w^{\beta-b-j}, \tag{5.4}$$

the second sum on the right being omitted when $\beta = b$, as indicated by the limits. By (5.3), (5.4) is equivalent to

$$(w-\gamma_1)(w-\gamma_2)\cdots(w-\gamma_\beta) \equiv w^{\beta-b}(w-c_1)(w-c_2)\cdots(w-c_b),$$

which proves the theorem. (In this proof we have not assumed the fundamental theorem of algebra in its $\mathfrak{F}_c$ form, but have used the abstractly identical consequences in $\mathfrak{A}$ of this theorem, necessary for the above inference, in the form given by Kronecker. An accessible introductory account of the relevant algebra is given in Wedderburn's paper on Fields in the *Annals of Mathematics* 1922.)

Let next $z \equiv (z_1, \cdots, z_n)$ be a matric variable of order n in $\mathfrak{A}$; let the c_{ik}, $\gamma_{jk}\,(i = 1, \cdots, b;\ j = 1, \cdots, \beta;\ k = 1, \cdots, n)$ be scalars, and for $m = 0, 1, \cdots$ write

$$C_i \equiv (c_{i1}, c_{i2}, \cdots, c_{in}), \qquad \Gamma_j \equiv (\gamma_{j1}, \gamma_{j2}, \cdots, \gamma_{jn}),$$

$$S_m \equiv (C_1 z)^m + \cdots + (C_b z)^m, \qquad \Sigma_m \equiv (\Gamma_1 z)^m + \cdots + (\Gamma_\beta z)^m,$$

where $(uz)^m$ is the mth power of the scalar product (uz). We shall prove that

$$S_m = \Sigma_m \qquad (m = 1, \cdots, \beta) \tag{5.5}$$

implies that $\beta - b$ *of the* Γ_j *are each equal to* $(0)_n$ (the zero matrix of order n in $\mathfrak{A}$), *and that the remaining* b *of them are a permutation of the* $C_i\,(i = 1, \cdots, b)$.

For, by the lemma just proved it follows from (5.5) that $\beta - b$ of the $(\Gamma_j z)$ $(j = 1, \cdots, \beta)$ vanish and that the remaining b are a permutation of $(C_i z)$ $(i = 1, \cdots, b)$. But a particular $(\Gamma_j z)$, say $(\Gamma_r z)$, since z is a matric variable, vanishes only with Γ_r, that is, only when $\Gamma_r = (0)_n$. Further, a particular pair of the $(\Gamma_j z)$, $(C_i z)$ are equal, say $(\Gamma_p z) = (C_q z)$, only when $\Gamma_p = C_q$, for the same reason; which is the theorem.

Observe now that S_{2m} is the sum of the mth powers of the squares of the $(C_i z)$ $(i = 1, \cdots, b)$, and similarly for Σ_{2m}. Hence, by the last lemma, if

$$S_{2m} = \Sigma_{2m} \qquad (m = 1, \cdots, \beta), \tag{5.6}$$

we reach a conclusion regarding the $(C_i z)^2$, $(\Gamma_j z)^2$ $(i = 1, \cdots, b;$ $j = 1, \cdots, \beta)$ precisely similar to that which follows from (5.5) for the $(C_i z)$, $(\Gamma_j z)$. Since z is a matric variable we have then the chain of implications,

$$\begin{aligned}
(\Gamma_p z) &= (C_q z) \ :\supset: \ \Gamma_p &&= C_q;\\
(\Gamma_p z)^2 &= (C_q z)^2 \ :\supset: \ (\Gamma_p z) &&= \pm (C_q z),\\
&\qquad\quad :\supset: \ \Gamma_p &&= \pm C_q,\\
&\qquad\quad :\supset: f(\Gamma_p\,|\,) &&= f(C_q\,|\,),
\end{aligned}$$

where $f(z\ )$ is a parity function, of parity $p(n\,|\,0)$ in the scalar variables of z, or $p((1\,|\,0))$ in z.

Without loss of generality let the $\beta - b$ vanishing Γ_r be Γ_t $(t = 1, \cdots, \beta - b)$. Then, from what precedes, it follows that (5.6) implies

$$\sum_{i=1}^{b} f(C_i\,|\,) = \sum_{j=1}^{\beta-b} f((0)_n\,|\,) + \sum_{\beta-b+1}^{\beta} f(\Gamma_j\,). \tag{5.7}$$

The last has an immediate and useful extension. Let the c_p be integers, and write

$$k = |c_1| + |c_2| + \cdots + |c_t|\,.$$

Then, by suitable transpositions,

$$\sum_{p=1} c_p\,(C_p\,z)^{2m} = 0 \qquad (m = 1, \cdots, k) \tag{5.8}$$

can be reduced to a relation of the form (5.6), to which we can apply the lemma proved for (5.7). By retranspositions in an obvious way to a form corresponding to (5.8) the final result of this application of (5.7) shows that (5.8) implies

$$\sum_{p=1}^{t} c_p f(C_p|) = 0. \tag{5.9}$$

Let the c_p be as above, and let c be an integer. If

$$\sum c_p = c, \tag{5.10}$$

we may consider, in the following proof, $c \geqq 0$; for if $c < 0$ it suffices to change signs throughout (5.10). Applying the results already proved we shall obtain the *first principal lemma*: (5.8) *and* (5.10) *together imply*

$$\sum_{p=1}^{t} c_p f(C_p|) = c f((0)_n|). \tag{5.11}$$

The coefficients c_p, c, by the above remark, are any rational integers. By an obvious extension these coefficients may be any numbers in $\mathfrak{F}_r$, for the latter case is reduced to the former on first clearing of fractions in (5.8), (5.10), and finally, in the statement deduced from these by the first principal lemma, corresponding to (5.11), dividing throughout by the common denominator used in the first step.

It will be sufficient to outline the steps by which this lemma is reduced to the preceding. By transpositions, if necessary, and by an application of the remark on (5.10), also by writing $c_p = 1+1+\cdots+1$ (p times), or the negative of this if $c_p < 0$, the hypothesis is reduced to the form which implies (5.7). By reversing the above transpositions and resolutions of coefficients into sums of units, we recover from the equality corresponding to (5.7) the required (5.11).

The first principal lemma is implied by the eveness of the exponents $2m$ ($m = 1, \cdots, k$) in (5.8), and it may be anticipated that

$$\sum_{p=1}^{t} c_p (C_p z)^{2m+1} = 0 \qquad (m = 1, \ldots, k) \tag{5.12}$$

implies (corresponding to (5.11))

$$\sum_{p=1}^{t} c_p f(C_p) = 0, \tag{5.13}$$

where the parity function $f(z)$ has parity $\rho(0\ n)$ (or $\rho((0\ 1))$ in z), but I have not proved this in $\mathfrak{A}$. I shall therefore circumvent its use in proving the principle of paraphrase in $\mathfrak{F}_r$ by making all instances of which (5.13) is the type depend upon (5.11).

On account of its interest we conclude these lemmas with a purely algebraic theorem, due to Professor C. F. Gummer, which can be taken as a basis for proving the first principal lemma in $\mathfrak{F}_c$ or $\mathfrak{F}_r$.

It was shown by Laguerre that the real equation

$$a_1 x^{n_1} + a_2 x^{n_2} + \cdots = 0,$$

in which the n_j are rational and $n_1 > n_2 > \cdots$, has not more roots > 1 than the number of variations of sign in the sequence

$$a_1, \quad a_1 + a_2, \quad a_1 + a_2 + a_3, \quad \cdots.$$

and the proof of this theorem can be extended to irrational n_j. Let $x = e^{\xi}$, $n_j = \log_e c_j$, $c_j > 0$. Then it follows that

$$\sum_1^p a_j c_j^{\xi} = 0.$$

has not more positive roots in ξ than the number of variations in the sequence. Hence, if the b_j, c_j are positive,

$$\sum_1^p b_j^{\xi} = \sum_1^p c_j^{\xi}$$

is not true for more than $p - 1$ positive integers ξ unless it is an identity.

6. Application of the circular functions in $\mathfrak{A}$. It is easily seen that $\mathfrak{P}$ can be obtained by operations in $\mathfrak{B}$ or $\mathfrak{C}$

from the circular functions in $\mathfrak{A}$ in a manner abstractly identical with that which is sometimes used to derive $\mathfrak{T}$ from the power series expansions of the sine and cosine in $\mathfrak{F}_c$ or $\mathfrak{F}_r$. If x is in $\mathfrak{A}$, we define $\sin x$, $\cos x$, by

$$\cos x = \sum_0^\infty (-1)^n \frac{x^{2n}}{(2n)!}, \qquad \sin x = \sum_0^\infty (-1)^n \frac{x^{2n+1}}{(2n+1)!};$$

and the operations by which such functions are combined to yield $\mathfrak{T}$ in $\mathfrak{A}$ are in either $\mathfrak{B}$ or $\mathfrak{C}$, preferably the former, see chapter I § 22. If $\mathfrak{A}$ is replaced by either of its instances $\mathfrak{F}_j$ $(j = c, r)$, these functions and all operations upon them are as in common analysis; in $\mathfrak{A}$ they have no numerical significance.

We recall that $(z\,w)$ is the scalar product of the matric variables z, w, and that $\varphi((z\,w))$ is written $\varphi(z\,w)$. With the notation of (5.11) for C_p, z we have the following. *If*

$$\sum_{p=1}^{t} c_p \cos(C_p z) = c \tag{6.1}$$

is an identity in z, so that (6.1) *holds for all values of the independent variables $z_j (j = 1, \cdots, n)$ in z, then* (6.1) *implies* (5.11).

For, if in (6.1) we replace z by tz, where t is a scalar parameter, and equate coefficients of like powers of t, we recover (5.8), (5.10), which together imply (5.11).

Note that by equating coefficients of t^{2m} $(m = 0, 1, \cdots)$ we get in addition to the relations required for the proof an infinity more which are unnecessary. The superfluous relations are implied by the necessary, as may be shown by the lemma just proved or independently. Thus the cosine identity (6.1) is sufficient but not necessary for the proof of (5.11), and this appears to be the algebraic equivalent of the analytical concept of type excess for functions in § 4.

Now by decomposition in $\mathfrak{T}$ each of (3.21) and (3.11), (3.31), provided in the last two that s be even, can be reduced to the form (6.1), from which follows the corresponding (5.11). From the last, by the identical transformation in $\mathfrak{P}$ abstractly identical with the expansion formula in $\mathfrak{T}$

which in each restores the decompositions in $\mathfrak{T}$ to the functions decomposed, *we infer the principle of paraphrase in* § 3 *for* (3.22) *in all cases, and for* (3.12), (3.32) *in those cases when* $s = \delta_1$ *is even, in the extended form in which the* α, β *matrices in* $\mathfrak{A}$.

There remains then only (3.32) with s odd, since evidently (3.12) with s even is reducible by the identical algorithm in $\mathfrak{P}$ to dependence on (3.32). *At this point we pass from* $\mathfrak{A}$ *to its instance* $\mathfrak{F}_r$.

The proof for $\mathfrak{F}_r$ is easily completed by applying the identical algorithm in $\mathfrak{P}$ to the following remarks. From the definition (§ 2) of parity functions, such a function $f(\mid z_1, \cdots, z_n)$, of parity $p(0 \mid 1^n)$ in the variables $z_j (j = 1, \cdots, n)$, is equivalent to $(z_1 z_2 \cdots z_n) f(z_1, z_2, \cdots, z_n \mid)$, where $f(z_1, \cdots, z_n \mid)$ is a parity function, of parity $p(1^n \mid 0)$. Consider now the instance of (3.31), (3.32) in which the absolute parity of h, indicated in (3.02), is the special one $p(0 \mid 1^s)$. Each matric variable in h is now of order 1. By partial differentiations with respect to each of the s independent variables now in (3.31) in turn the $\mathfrak{T}$ identity (3.31) is reduced to a cosine form to which the preceding result can be applied immediately. Each term in the paraphrase is of the form $c\beta_1 \beta_2 \cdots \beta_s f(\beta_1, \beta_2, \cdots, \beta_s \mid)$, $\equiv c f(\mid \beta_1, \beta_2, \cdots, \beta_s)$, by the first remark. The above algebra is legitimate if and only if the $\beta_j (j = 1, \cdots, s)$ are rational integers as assumed. Hence the paraphrase of (3.31) into (3.32) is proved in the special case when h in (3.32) is of parity $p(0 \mid 1^s)$. Thence, by the identical algorithm in $\mathfrak{P}$, the general (3.22) is established on observing that in any $\mathfrak{T}$ identity whose right hand member is zero, obtained by expansion, the set of all terms having a given parity vanishes independently of the remaining terms.

Hence we have proved the principle in § 3 in all cases, and we have extended it from $\mathfrak{F}_r$ to $\mathfrak{A}$ for parity functions whose odd degress δ_1 ($\equiv s$ in the notation of § 2) are even integers > 0. As already remarked it seems highly probable that the extension to $\mathfrak{A}$ holds also when δ_1 is odd, but this has not been proved.

EXTENSION OF THE PRINCIPLE TO HIGHER FORMS, §§ 6-11

6.1. Odd and even algebraic forms. We shall say that the matric variable $z \equiv (z_1, \cdots, z_r)$ of order r has an *integral value* when and only when the $z_j (j = 1, \cdots, r)$ are rational integers. Thus the α_{ik}, β_{jk} $(i = 1, \cdots, r;$ $j = 1, \cdots, s;$ $k = 1, \cdots, n)$ in (3.12)–(3.32) are integral values of the matric variables ξ_i, η_j in (3.01). The notation ω, ω_0, ω_1, ξ_i, η_j, $\cdots$ in what follows is as in § 3.

A rational integral algebraic function, not necessarily homogeneous, in k indeterminates with rational integral coefficients will be called a *form of order* k. Forms of preassigned orders and parities can easily be constructed. For example, the indeterminates being the x, y with suffixes occurring in the ξ_i, η_j, we get from (3.11) the form

$$\sum_{k=1}^{n} \left\{ q_k \prod_{i}^{r} {}_{1} (\alpha_{ik} \xi_i)^{2u_i} \prod_{j=1}^{s} (\beta_{jk} \eta_j)^{2v_j + 1} \right\} \tag{6.1}$$

having the order ω and the parity $p(a_1, \cdots, a_r \; b_1, \cdots, b_s)$; from (3.31),

$$\sum_{k=1}^{n} \left\{ l_k \prod_{i=1}^{r} (\alpha_{ik} \xi_i)^{2u_i} \right\}, \tag{6.2}$$

a form of order ω_0 and parity $p(a_1, \cdots, a_r \;)$; from (3.31),

$$\sum_{k=1}^{n} \left\{ t_k \prod_{j=1}^{s} (\beta_{jk} \eta_j)^{2v_j + 1} \right\}, \tag{6.3}$$

a form of order ω_1 and parity $p(\; b_1, \cdots, b_s)$, in all of which u_i, $v_j (i = 1, \cdots, r;$ $j = 1, \cdots, s)$ are arbitrary integers $\geqq 0$, the $(\alpha_{ik} \xi_i)$, $(\beta_{jk} \eta_j)$ are scalar products as always, and in (6.1), (6.3) β_{ik} is different from the zero matrix of order $b_j (j = 1, \cdots, s)$ in $\mathfrak{F}_r$. By expansion and decomposition in $\mathfrak{T}$ we can write down from (3.11)–(3.31) any number of forms having assigned orders, degrees $(\delta, \delta_0, \delta_1)$ and parities.

Let A be any form of order ω whose indeterminates are the x, y with suffixes occurring in the matric variables ξ_i,

$\eta_j (i = 1, \cdots, r;\ j = 1, \cdots, s)$. Then if in the ξ_i, η_j this form has the first of the parities (3.02), we shall write

$$A \equiv A(\xi_1, \cdots, \xi_r \mid \eta_1, \cdots, \eta_s),$$

which is said to be *even* in each of $\xi_i (i = 1, \cdots, r)$, *odd* in each of $\eta_j (j = 1, \cdots, s)$. Similarly for the forms B, C,

$$B \equiv B(\xi_1 \cdots, \xi_r \mid), \qquad C \equiv C(\mid \eta_1, \cdots, \eta_s),$$

of the respective orders ω_0, ω_1. even in each of the ξ_i, odd in each of the η_j respectively. Since A, B, C are instances of parity functions the algebra $\mathfrak{P}$ applies to them. In particular an arbitrary form can always be represented as a linear homogeneous function of forms having parity. In general a form has no parity; those having odd parities, $p(\ b_1, \cdots, b_s)$ are of special importance in the applications of the principle of paraphrase.

7. **Compound representation.** Let z' be an integral value of the matric variable $z \equiv (z_1, \cdots, z_r)$ of order r. Then, without loss of generality (see chapter I, § 9), any form $A(z_1, z_2, \cdots, z_r)$ in the r indeterminates $z_j (j = 1, \cdots, r)$ may be considered as a function of z, and it may be written $A(z)$. If z' is such that $A(z') = n$, the integer n is said to be *represented in* $A(z)$ by z'; if no integral value z'' of z exists such that $A(z'') = n$, then n is said to be *not represented in* $A(z)$.

Let now $A(z)$ be odd in z, so that we may write $A(z) \quad A(\mid z)$, and let $A[n]$ denote 1 or 0 according as n is or is not represented in $A(\mid z)$. Then $A[n] = A[-n]$. For if n is represented in $A(\mid z)$ by z', so that $A(\mid z') = n$, then $-A(\mid z') = A(\mid -z') = -n$ gives the representation of $-n$ in $A(\ z)$ by $-z'$. If next n is not represented in $A(\ z)$, if possible let z' be a representation of $-n$, so that $A(\mid z') = -n$. Then, by what precedes, $-z'$ is a representation of n, contrary to hypothesis. Again, since $A[n] = A[-n]$, and $A[x]$ takes a definite value for each integral value of the indeterminate x, it follows that $A[x]$ is a parity function having the absolute

parity $p(1\,|\,0)$, and we may write $A[x] \equiv A[x\,|\,]$. Hence *the function* $A[x\,|\,]$ *of the indeterminate* x, *which takes only the values* 0,1 *for integral values of* x, *and which is such that* $A[n\,|\,] = 0,\ 1$ *according as the integer* n *is or is not represented in the odd form* $A(\,|\,z)$ *of order* r, *is a parity function of* x *having the parity* $p(1\,|\,0)$.

With $z \equiv (z_1, \cdots, z_r)$ as above, let $A_j(\,|\,z)$ $(j = 1, \cdots, r)$ denote odd forms, each having the relative parity $p(\,z)$ as indicated by the notation, of the respective orders ω_j $(j = 1, \cdots, r)$, so that $A_j(\,|\,z)$ is a form in precisely ω_j of the z_j, $0 < \omega_j \leqq r$ $(j = 1, \cdots, r)$. For example, if $r = 3$, and $z = (u, v, w)$, where u, v, w are the variables, each of

$$A_1(\,|\,z) = au^m, \quad A_2(\,|\,z) = au^m + bv^s, \quad A_3(\,|\,z) = cu^p v^q w^t,$$

where a, b, c, m, s, p, q, t are integers > 0, and $m, s, p+q+t$ are odd, has the relative parity $p(\,|\,z)$.

Proceed in the same way with the matric variable $w \equiv (w_1, \cdots, w_s)$ of order s, and let $B_j(\,|\,w)$ be an odd form of order $\omega_j'(j = 1, \cdots, r)$. Note that r, s are not necessarily equal. Then for each integral value z' of z each of $A_j(\,z')$ $(j = 1, \cdots, r)$ is a definite integer. Hence $A_j(\,|\,z')$ is an appropriate argument for $B_j[x\,]$, and $B_j[A_j(\,z)\,|\,]$, considered as a function of z, is a parity function having the relative parity $p(z\,|\,)$. For, first, this function takes a single definite value for each integral value z' of z, since $B_j[A_j(\,|\,z')\,] = 1$ or 0 according as the integer $A_j(\,z')$ is or is not represented in the odd form $B_j(\,|\,w)$ of order ω_j'. Second,

$$B_j[A_j(\,|\,-z)\,|\,] = B_j[-A(\,|\,z)\,|\,] = B_j[A_j(\,|\,z)\,|\,],$$

since for each integral value of z either both or neither of $A_j(\,\pm z) = \pm A_j(\,z)$ do or do not represent a definite integer which is representable in $B_j(\,|\,w)$. Write

$$BA(z\,|\,) \equiv \prod_{j=1}^{r} B_j[A_j(\,|\,z)\,|\,].$$

Then, as above, it is easily seen that $BA(z|)$ is a parity function of z having the relative parity $\rho(z)$, and further that $BA(z|)$ takes only, for each integral value z' of z, a definite one of the values 0, 1. According as $BA(z'|) = 1$ or 0 we shall say that z' has or has not a *compound representation in the odd form matric variable of order* $2r$,

$$(B_1(|w),\ A_1(|z),\ B_2(|w),\ A_2(|z),\ \cdots,\ B_r(|w),\ A_r(|z)),$$

and the *compound order* of the last is the matrix

$$(\omega_1',\ \omega_1,\ \omega_2',\ \omega_2,\ \cdots,\ \omega_r',\ \omega_r).$$

For one choice of the $B_i(|w)$, $A_i(|z)$ the value of $BA(z|)$ is unity for all integral values z' of z; it suffices to take $B_i(|w) = w_i$, $A_i(|z) = z_i$ $(i = 1, \cdots, r)$. Call this the *unitary* $BA(z|)$ and write it $U(z|)$.

What follows is merely to simplify the writing of formulas when several w, z are involved in the same discussion. Assuming that for given matric variables w, z of any respective orders s, r the specific odd forms $B_i(|w)$, $A_i(|z)$ $(i = 1, \cdots, r)$ and their orders (in the above symbol of compound order) have been stated for a given compound representation indicated by $BA(z|)$, we shall write

$$BA(z|) \equiv K(z|),$$

whatever the matric variable z, and hence $K(z|) = 1$ or 0 according as z has or has not a compound representation in a certain odd form matric variable, of given order and given compound order. If ξ, η are distinct matric variables, $K(\xi|)$, $K(\eta|)$ do not therefore (in general) refer to compound representations in the same odd form matric variable, although, if ξ, η are of the same order, this possibility is not excluded when $K(\xi|)$, $K(\eta|)$ occur in the same context. In short the compound representation for which $K(\zeta|)$ is significant is arbitrary in the widest sense consistent with the definitions, and $K(\zeta|)$ has the relative parity $\rho(\zeta|)$ in the matric variable ζ.

8. Application of compound representations to the principle in § 3. The ξ_i. η_j in what follows are as in § 3. The absolute parities of

$$\prod_{i=1}^{r} K(\xi_i|) \prod_{j=1}^{s} K(\eta_j|), \qquad \prod_{i=1}^{r} K(\xi_i|), \qquad \prod_{j=1}^{s} K(\eta_j|)$$

are respectively

$$\begin{matrix} p(a_1, \cdots, a_r, b_1, \cdots, b_s|0), \\ p(a_1, \cdots, a_r|0), \quad p(b_1, \cdots, b_s|0). \end{matrix} \tag{8.1}$$

Hence we shall abbreviate these products to

$$K(\xi_1, \cdots, \xi_r, \eta_1, \cdots, \eta_s), \quad K(\xi_1, \cdots, \xi_r), \quad K(\eta_1, \cdots, \eta_s).$$

The following products

$$\begin{matrix} K(\xi_1, \cdots, \xi_r, \eta_1, \cdots, \eta_s|) f(\xi_1, \cdots, \xi_r|\eta_1, \cdots, \eta_s), \\ K(\xi_1, \cdots, \xi_r|)\, g(\xi_1, \cdots, \xi_r|), \\ K(\eta_1, \cdots, \eta_s|)\, h(|\eta_1, \cdots, \eta_s) \end{matrix} \tag{8.2}$$

have the respective parities (3.02); we shall write them, corresponding to (3.01), as

$$Kf(\xi_1, \cdots, \xi_r|\eta_1, \cdots, \eta_s), \quad Kg(\xi_1, \cdots, \xi_r|), \quad Kh(|\eta_1, \cdots, \eta_s), \tag{8.3}$$

or shorter, Kf, Kg, Kh.

These three functions are instances of f, g, h respectively in (3.01), *and conversely, if* $K(\xi_i)$, $K(\eta_j|)$ $(i = 1, \cdots, r;$ $j = 1, \cdots, s)$ *in* Kf, Kg, Kh *be replaced by the unitaries* $U(\xi_i|)$, $U(\eta_j|)$ *respectively,* f, g, h *are recovered from* Kf, Kg, Kh.

Apply this to (3.11)–(3.33). *Then* (3.11)–(3.31) *imply* (3.12)–(3.22) *in which* f, g, h *are replaced by* Kf, Kg, Kh, *and conversely, the* Kf, Kg, Kh *form of* (3.12)–(3.32) *implies the* f, g, h *form.* That is, *the* f, g, h *and the* Kf, Kg, Kh *forms of* (3.12)–(3.32) *are formally equivalent, and they are implied by* (3.11)–(3.31) *respectively.*

The effect of this extremely general transformation upon the algebraic arithmetic of the multiply periodic functions will

be examined after we have considered the next, which introduce arbitrary even forms into the principle of paraphrase.

9. Limited representations. Let $z = (z_1, \cdots, z_r)$ be a matric variable of order r, and let $A_k(z|)\ (k = 1, \cdots, t)$ be even forms of order $\omega_k \leqq r$; so that $A_k(z|) = A_k(-z|)$, and $A_k(z|)$ is an even form in precisely $\omega_k\ (k = 1, \cdots, t)$ of the indeterminates $z_j\ (j = 1, \cdots, r)$. Let the α_k, β_k $(k = 1, \cdots, t)$ be constant real numbers, and z' an integral value of z. Then $A_k(z'|)$ is a definite integer. Let $\{x\}$ denote 1 or 0 according as $\alpha_k \leqq x \leqq \beta_k$ is true or false for the integer x. Then $A_k(z\ )$ is an admissible argument x for $\{x\}$, and $\{A_k(z|)\} = \{A_k(-z)\}$, so that we may write

$$\{A_k(z|)\} \equiv A_k\{z|\}\ (k = 1, \cdots, t)$$

and $A_k\{z\ \}$ is a parity function of z having the relative parity $p(z|)$. The product

$$L(z\ ) \equiv \prod_{k=1}^{t} A_k\{z\ \}$$

is therefore a parity function of z having the relative parity $p(z|)$, and $L(z'|) = 1$ *if simultaneously*

$$\alpha_k \leqq A(z'|) \leqq \beta_k \qquad (k = 1, \cdots, t),$$

while if one (or more) of these t inequalities is false, $L(z'\ ) = 0$.

In a way similar to that in § 7 we regard the t specific even forms $A_k(z|)$ and the t pairs of limiting values α_k, β_k $(k = 1, \cdots, t)$ as being explicitly given, although not indicated in the notation, when an $L(z\ )$ is written for any matric variable z of order r and, as in § 7, when z, w are distinct matric variables of the same or different orders, it is not assumed either that any limit or that any even form to which $L(z\ )$ refers is the same as the like for $L(w|)$, or that the t's for the two are the same.

If in $L(z|)$ as defined, $t = r$, $A_k(z|) \equiv z^2\ (k = 1, \cdots, r)$, and $\alpha_k = 0$, $\beta_k = \infty\ (k = 1, \cdots, r)$, we get $L(z'|) = 1$ for

every integral value z' of z. We shall call this special case the *unitary* $L(z|)$ for the matric variable z, and write it $V(z|)$.

Precisely as in § 8 we now (with the same ξ_i, η_j as there) construct

$$\prod_{i=1}^{r} L(\xi_i|) \prod_{j=1}^{s} L(\eta_j|), \qquad \prod_{i=1}^{r} L(\xi_i), \qquad \prod_{j=1}^{s} L(\eta_j),$$

which have the respective absolute parities (8.1), and shorten these to

$$L(\xi_1, \cdots, \xi_r, \quad \eta_1, \cdots, \eta_s|), \quad L(\xi_1, \cdots, \xi_r|), \quad L(\eta_1, \cdots, \eta_s|).$$

Corresponding to (8.2), on replacing therein K by L, we obtain

$$Lf(\xi_1, \cdots, \xi_r|\eta_1, \cdots, \eta_s), \quad Lg(\xi_1, \cdots, \xi_r|), \quad Lh(|\eta_1, \cdots, \eta_s),$$

or in shorter form Lf, Lg, Lh, corresponding to (8.3), and see that *these three functions are instances of* f, g, h *respectively in* (3.01), *and conversely, if* $L(\xi_i|)$, $L(\eta_j|)$ $(i = 1, \cdots, r;\ j = 1, \cdots, s)$ *in* Lf, Lg, Lh *are replaced by the unitaries* $V(\xi_i)$, $V(\eta_j)$ *respectively,* f, g, h *are recovered from* Lf, Lg, Lh.

According as $L(z'|) = 1$ or 0 we shall say that z' (= integral value of the matric variable z) has or has not a *limited representation*, the latter being defined by the specific pairs of limiting values α_k, β_k and the even forms $A_k(z)$ $(k = 1, \cdots, t)$ which define $L(z|)$.

10. Application of limited representations to the principle in § 3. Since Lf, Lg, Lh are instances of f, g, h respectively in (3.01) we see that (3.11)–(3.31) *imply* (3.12)–(3.32) *in which* f, g, h *are replaced by* Lf, Lg, Lh, *and conversely (by passing to unitary* L's*) the* Lf, Lg, Lh *form of* (3.12)–(3.32) *implies the* f, g, h *form. Hence both the* f, g, h *and the* Lf, Lg, Lh *forms of* (3.12)–(3.32) *are implied by* (3.11)–(3.31), *and they are formally equivalent.*

11. Limited compound and compound limited representations. We now consider the simultaneous effects of L, K and of K, L in these orders (the results are not

the same in general), on f, g, h as in (3.01) and their significance for the general principle in § 3.

The α, β with suffixes in (3.12)–(3.32) are $r+s$ integral values of the matric variables ξ_i, η_j, of the respective orders a_i, b_j, $(i = 1, \cdots, r;\ j = 1, \cdots, s)$. Hence, through the α, β, there are involved in the f, g, h in (3.12)–(3.32) precisely $n\omega$, $n\omega_0$, $n\omega_1$ integers, where ω, ω_0, ω_1 are as defined in § 3. Let us consider the case which actually occurs in connection with the n fold $(n > 1)$ periodic functions. The $n\omega$, $n\omega_0$, $n\omega_1$ integers just described are linear functions $\lambda_1, \lambda_2, \cdots$ of the integers $\nu_1, \nu_2, \cdots$ which represent a set of constant integers $\varkappa_1, \varkappa_2, \cdots$ in a system $\mathfrak{S}$ of forms (as defined in § 6) of the second degree, that is, each member of $\mathfrak{S}$ is a quadratic (not necessarily homogeneous) form or a bilinear form. For example, $\mathfrak{S}$ may consist of the single form

$$\nu_1^2 + 2\nu_2^2 + 3\nu_3^2 + 6\nu_4^2 \cdots = f(\nu_1, \nu_2, \nu_3, \nu_4);$$

the $\lambda_1, \lambda_2, \cdots$ may then be of the type $c_1\nu_1' + c_2\nu_2' + c_3\nu_3' + c_4\nu_4'$, where the c's are integers not all zero, the ν_i' being determined, for example, by a set of equations each of the type $f(\nu_1', \nu_2', \nu_3', \nu_4') = \varkappa$ where $\varkappa$ is a constant integer, and finally the $\lambda_1, \lambda_2, \cdots$, or certain of them, are the integers from which the α, β (with suffixes) are constructed. Examples will be given later in this chapter; for the present it is sufficient to note that the λ's are linear in the indeterminates defined by $\mathfrak{S}$, and that each form in $\mathfrak{S}$ is only of the second degree. We shall say that each of (3.12)–(3.32) is *integrated over* $\mathfrak{S}$.

If in (3.12)–(3.32) we replace f, g, h by Lf, Lg, Lh, we thereby select from the λ's only such as satisfy certain limiting conditions or, by an obvious analogy, the f, g, h theorems are integrated over the whole of $\mathfrak{S}$ and the Lf, Lg, Lh over only a limited region $\mathfrak{S}_L$ of $\mathfrak{S}$. The conditions imposed by L can, in certain instances, depending upon the specific even forms appertaining to L, be transferred directly to $\mathfrak{S}$. *Having restated* (3.12)–(3.32) *in reference to* L, *which can always be done explicitly by merely adjoining to* $\mathfrak{S}$ *the set of*

inequalities imposed by L and retaining the f, g, h forms of (3.12)–(3.32), *we can then apply K to the result.* The effect of K upon the f, g, h forms of (3.12)–(3.32) is again the adjunction of a further set of indeterminate equations to those of $\mathfrak{S}$. If the forms appertaining to K are sufficiently simple (for example, if each is a constant times a single arbitrary odd power of one indeterminate) we can omit reference to $\mathfrak{S}$ after transforming it to a system $\mathfrak{S}_K$ of forms of degree >2 by means of K. In all cases the application of L, K introduces forms of higher degree than the second. Proceeding in the same way with $\mathfrak{S}_L$ and K, we restate (3.12)–(3.32) with reference to $\mathfrak{S}_{LK}$, in which L is applied first, and similarly for $\mathfrak{S}_{KL}$. Taking now either the same or different K, L we can start from $\mathfrak{S}_{LK}, \mathfrak{S}_{KL}$, and derive paraphrases integrated over

$$\mathfrak{S}_{LL}, \mathfrak{S}_{LLK}, \mathfrak{S}_{KLK}, \mathfrak{S}_{KKL}, \cdots,$$

and so on indefinitely. *In this way we escape from the traditional limitation to forms of degree $\neq 2$ of the applications of the elliptic and other periodic functions to algebraic arithmetic.* It is to be noticed that *the odd or even degree of any form concerned is an arbitrary constant odd or even integer.* The applications are so numerous, and so readily made, that we shall take space in the following for only a few of the simplest to show their nature.

APPLICATION OF THE PRINCIPLE TO THETA QUOTIENTS, §§ 12–16

12. Arithmetical expansions of theta quotients. We shall indicate a few of the more prolific sources from which arithmetical expansions (see § 1) can be derived. Of the first importance in the present connection are the doubly periodic functions of the second kind, $\varphi_{\alpha\beta\gamma}(x, y)$, where $\vartheta_\alpha(x) \equiv \vartheta_\alpha(x, q)$ $(\alpha = 0, 1, 2, 3)$,

$$\varphi_{\alpha\beta\gamma}(x, y) = \frac{\vartheta_1' \vartheta_\alpha(x+y)}{\vartheta_\beta(x)\vartheta_\gamma(y)} \equiv \varphi_{\alpha\beta\gamma}(x, y, q),$$

for the following 16 values of the triple index $\alpha\beta\gamma$,

$$\begin{array}{cccc} 001, & 010, & 023, & 032, \\ 100, & 111, & 122, & 133, \\ 203, & 212, & 221, & 230, \\ 302, & 313, & 320, & 331, \end{array}$$

as by means of them we introduce in the simplest way parity functions in matric variables of any orders > 1 whose several arguments contain the divisors $d_1, d_2, \cdots$ of a set of integers $n_1, n_2, \cdots$ *and their conjugates,* $\delta_1, \delta_2, \cdots$, namely we have $d_1\delta_1 = n_1$, $d_2\delta_2 = n_2, \cdots$. The doubly periodic functions of the first kind (elliptic functions) do not in general give rise to such parity functions without the use of elaborate reductions by means of the arithmetical theory of quadratic and bilinear forms, all of which are avoided by the simple analysis of the expansions. Accurate forms of these are given in the *Messenger of Mathematics*, vol. 49 (1919), p. 83. A typical one is

$$\varphi_{331}(x, y) = \csc y + 4\sum q^n\left[(-1)^n \sum \sin(2tx + \tau y)\right],$$

in which the first $\sum$ refers to $n = 1, 2, 3, \cdots$, the second to all pairs (t, τ) of integers $t, \tau > 0$, of which τ is odd, such that $t\tau = n$. The same list is also given, with a less convenient notation for the divisors, in the *Transactions*, vol. 22 (1921) p. 207. The entire literature of the expansions of theta quotients (in the usual analytical forms) seems to have been singularly unfortunate in the matter of misprints; Jacobi's collected works however are an exception.

From the above 16 can be derived by elementary methods a great number of reduced arithmetical expansions for powers and products of elliptic functions and for the doubly periodic functions of kinds higher than the second. A selection is given in the *Quarterly Journal*, vol. 54 (1924), pp. 166–176; the few misprints can be easily corrected by means of the outline of the method used.

The principal sources for expansions of functions of the third kind, all of the greatest interest for arithmetic when

reduced to their proper forms, are Hermite's *Œuvres*, the Thèse of Biehler *Sur les Developpements en séries des fonctions doublement periodiques de troisième espèce*, Paris 1879, the papers of Appell in the *Annales . . . de l'École normale superieure*, vol. 1 (1884), pp. 135–164; vol. 2, pp. 9–36, 67–74; vol. 3, pp. 9–42; vol. 5, pp. 211–218, also *Acta Mathematica*, vol. 42 (1920), pp. 341–347, and the series of papers by Krause, *Mathematische Annalen*, vol. 30 (1887), pp. 425–436, 516–534; vol. 32, pp. 331–341; vol. 33, pp. 108–118; vol. 35, pp. 577–587, also his treatise, *Doppeltperiodische Funktionen*, Leipzig 1895. Almost any one of these references offers an inexhaustible source of arithmetical theorems when subjected to the methods of this chapter.

The introduction of indefinite binary quadratic forms into theta expansions was first effected by Petr, although it is probable that certain theorems stated by Stieltjes were obtained by such means. The papers of Petr are in Czech: independently most of the fundamental expansions were found later by G. Humbert, *Journal des Mathématiques*, 6 ser., vol. 3 (1907), pp. 337–449. Humbert's 6 basic expansions are reduced to their arithmetical forms in the *Quarterly Journal*, vol. 49 (1923), p. 328. These are particularly suggestive in the theory of generalized class number relations. These few indications must suffice, as I hope on another occasion to consider the arithmetic of theta quotients from the present point of view in detail. Such expansions as are necessary for illustrations presently will be stated without further reference.

13. Elimination of negative powers of sines and cosines. Many of the arithmetical expansions contain terms in $\sec x$, $\csc x$, $\tan x$, $\cot x$, $\sec(x \pm y)$, $\tan(x \pm y \pm z)$, $\cdots$ etc. Such terms must always be eliminated from any identity I between circular functions obtained by equating coefficients of like powers of q in an identity between arithmetical expansions of theta quotients before proceeding to paraphrase. Let $\varphi(x)$ denote any one of $\sec x$, $\csc x$, $\tan x$, $\cot x$, and $\psi(y)$ either of $\sin y$, $\cos y$. Then any product of the form $\varphi(x)\,\psi(nx)$, where n is an integer, can be reduced to the form $A\varphi'(x) +$

a finite sum of sines or cosines of integral multiples of x, where $\varphi'(x)$ is a definite $\varphi(x)$ and A is independent of x, (A may $= 0$), by means of 16 formulas $\varphi(x)\ \psi(n,x)$, n even or odd, of which typical ones are

$$\cos 2nx \csc x = \csc x - 2\sum_{r=1}^{n} \sin(2r-1)x,$$

$$\cos(2n+1)x \sec x = (-1)^n\left[1 + 2\sum_{r=1}^{n}(-1)^r \cos 2rx\right].$$

If a power $\varphi^r(x)$, $r>1$ occurs, r applications of the appropriate ones of the 16 formulas effect the reduction. If a function of more than one variable, say $\varphi(x+y)\ \psi(n_1x+n_2y)$, where n_1, n_2 are integers, is to be reduced, we replace the argument of φ by a single variable, $z = x+y$, getting then $\varphi(z)\ \psi(n_1-n_2)x+n_2z)$. On expansion of the ψ factor by the addition formulas for sin, cos, the reduction is referred to the previous cases. The complete set of reduction formulas for 2 variables is given in the paper *Quelques applications ··· à trois termes* in the *Giornale di Matematiche*, vol. 59 (1921).

14. Applications of division of parities. From the examples given shortly many interesting consequences in the same number of variables or fewer may be derived by the methods of Chapter I, §§ 18-21, among which we note the following. Consider for example a relation of the type (3.32) with $h \equiv h(x, y, (z, r))$, where the x, y, z, r are independent variables. Since h is a parity function in (3.32), each of the parity functions $h_1(x, y, z)$, $h_2(x, y, r)$ may replace h in (3.32), since each satisfies the parity conditions upon h.

More generally, if any or all of the variables in any matric variable to the left of the bar be deleted in the symbol of a parity function, or if in any matric variable occurring to the right of the bar any number of variables less than the order of the matric variable concerned be suppressed, the resulting functions are instances of the original, and such transformations may be applied successively to deduce from a given (3.12)–(3.32) instances of the latter in fewer variables. Hence, the notation being as just after (3.02), we get in this

way from (3.12)–(3.32) respectively the following numbers of paraphrases concerning functions whose orders do not exceed the orders ω, ω_0, ω_1 of f, g, h,

$$2^{\omega-\delta_1}, \qquad 2^{\omega_0}, \qquad 2^{\omega_1-\delta_1},$$

including the case where the functions are constant (parity $p(0|0)$).

Again, further instances can be obtained by replacing the variables in any matric variable by a linear homogeneous function of themselves with integral coefficients, with the restriction that the coefficients be not all zero if the matric variable is to the right of the bar. This includes the instances just stated.

As another useful transformation, it is clear from the definition in § 2 that any common factor (in the sense of rational arithmetic) of all the integral values of a given matric variable in (3.12)–(3.32) may be suppressed.

Sums of functions transformed in any of the above ways, or linear homogeneous functions of them with integral coefficients are further instances.

We note finally the following among the numerous transformations leaving the truth of (3.12)–(3.32) unchanged. Certain of the variables, scalar or matric or both, in any (3.12)–(3.32) may be subjected to all the substitutions of a finite group G on them whence, by addition, are obtained arbitrary functions which have parity and which are invariants of G. This can be generalized to substitutions which change the signs of the functions, or which reproduce the functions multiplied by constants.

15. Consequences of Jacobi's theta formula. For the derivation of paraphrases from the theta quotients, Jacobi's memoir, *Theorie der elliptischen Funktionen*, *Werke*, vol. 1, pp. 499–538, is the most prolific source. Its arithmetical consequences have barely been noticed, and not at all in any systematic manner. We need give only a few instances.

The first arithmetical identities of the types (3.12)–(3.32) were stated by Liouville, who asserted that he had found

them by elementary means. Proofs for most of his formulas by such methods were given by later writers, references to whose papers will be found in Dickson's *History*, vol. 2, chapter XI. The entire set of Liouville's general formulas follow by the principle in § 3 from elementary transformations of Jacobi's theta identities, and these in turn are implied by Jacobi's formula for the multiplication of four theta functions. The same is necessarily true of Weierstrass' equation of three terms, since, as is well known, this equation is equivalent to Jacobi's formula. The formula itself (see Jacobi's proof) rests on the elementary identity which transforms a sum of 4 squares into itself, and all proofs by elementary means of arithmetical theorems of the types (3.12)–(3.32) amount to repeated applications of this transformation. It will be of interest to indicate briefly the analytical origins of those of Liouville's theorems for which algebraic proofs have not hitherto been published. The complete deduction of the theorems from the theta identities and expansions stated is a straightforward exercise in trigonometry.

As a first example let $\varphi(w, z, u, v)$ be a restricted parity function (see § 2) subject to the restrictions

$$\varphi(w, z, u, v) = -\varphi(-w, -z, -u, -v) = -\varphi(w, -z, v, u),$$

the first of which states merely that φ has the relative parity $p(|(w, z, u, v))$. Then, the $\sum$ referring to all sets of integers $\nu_1, \nu_2, \mu_3, \nu_4, \nu_5$ such that $\nu_1, \nu_2, \nu_4, \nu_5 \gtreqless 0$ are odd or even, $\mu_3 \gtreqless 0$ is odd, and for the constant $\alpha \equiv 1 \bmod 4$,

$$\alpha = 4\nu_1^2 + 4\nu_2^2 + \mu_3^2 + 4\nu_4^2 + 4\nu_5^2,$$

we have the following,

$$\sum (-1)^{\nu_1+\nu_5} (-1 \quad \mu_3)$$
$$\times [\varphi(2\nu_1+2\nu_2+\mu_3, \quad 2\nu_1-\mu_3-2\nu_4, \quad \nu_1-\nu_2, \nu_4+\nu_5)$$
$$+ \varphi(2\nu_1+2\nu_2+\mu_3, -2\nu_1+\mu_3-2\nu_4, -\nu_1+\nu_2, \nu_4+\nu_5)] = 0.$$

In this (as usual), $(-1\,|\,m) \equiv (1)^{(m-1)/2}$. In particular we may take $f(|(w, z, u, v))$, unrestricted of the indicated absolute parity $p(|(w, z, u, v))$, and choose

$$\varphi(w, z, u, v) \equiv f(|(w, z, u, v)) - f(|(w, -z, v, u)).$$

This is the most general φ satisfying the stated conditions. For the theorem is the immediate paraphase of the following theta identity which is easily deduced from those given by Jacobi,

$$[\Phi(w, u, z) + \Phi(w, -u, -z)]\, \vartheta_3(v-z)\, \vartheta_0(v)$$
$$= [\Phi(w, v, -z) + \Phi(w, -v, -z)]\, \vartheta_3(u+z)\, \vartheta_0(u),$$

where

$$\Phi(\lambda, \mu, \varrho) \equiv \vartheta_0(\lambda+\mu+\varrho)\, \vartheta_3(\lambda-\mu)\, \vartheta_1(\lambda-\varrho).$$

To introduce functions of the second kind into the identity divide throughout by $\vartheta_0(x+y)\, \vartheta_0(x-y)\, \vartheta_1(w+z)\, \vartheta_1(w-z)$ after replacing u, v by $x+y, x-y$ respectively. Then

$$\begin{aligned}
&\varphi_{001}(\ x+y,\ w+z)\, \vartheta_3(x-y-z)\, \vartheta_3(w-x-y)\\
&+\varphi_{001}(-x-y,\ w-z)\, \vartheta_3(x-y-z)\, \vartheta_3(w+x+y)\\
&-\varphi_{001}(\ x-y,\ w-z)\, \vartheta_3(x+y+z)\, \vartheta_3(w-x+y)\\
&-\varphi_{001}(-x+y,\ w+z)\, \vartheta_3(x+y+z)\, \vartheta_3(w+x-y) = 0
\end{aligned}$$

is an identity in x, y, z, w. The substitution for u, v is merely to enhance the symmetry of the final result. The expansion for φ_{001} is

$$\varphi_{001}(x, y) = \csc y + 4 \sum q^n \left[\sum \sin(2tx + \tau y)\right],$$

the outer $\sum$ referring to $n = 1, 2, 3, \cdots$, the inner to all pairs (t, τ) of divisors of n such that $n = t\tau$, $t, \tau > 0$, τ odd. Using this and

$$\vartheta_3(x) = \sum q^{\nu^2} \cos 2\nu x = 1 + 2 \sum q^{n^2} \cos 2nx$$
$$(\nu = 0, \pm 1, \pm 2, \cdots;\ n = 1, 2, 3, \cdots),$$

we get on comparing coefficients of like powers of q in the theta identity its paraphrase. Write

$$F(x, y, z, t) \equiv f(|x, y, (z, t)),$$

where f is unrestricted of the indicated parity $p(x, y, (z, t))$. Then, m being an arbitrary constant integer > 0, and the $\sum$

on the left of the following extending to all sets of integral solutions $(m_1, m_2, d_3, \delta_3)$ of

$$m = m_1^2 + m_2^2 + d_3\delta_3, \qquad m_1, m_2 \gtreqless 0, \quad \delta_3 \text{ odd}, \quad d_3, \delta_3 > 0,$$

and that on the right to $s = 0, 1, \cdots, a-1$ taken over all integral solutions (a, b) of

$$m = a^2 + b^2, \qquad a > 0,$$

the paraphrase is

$$\sum F(\delta_3 - 2m_2,\ d_3 + m_2 - m_1,\ d_3 + m_2 + m_1,\ \delta_3 + 2m_1) = \sum F(2a - 2s - 1,\ a - b,\ a + b,\ 2b + 2s + 1).$$

This is equivalent to Liouville's 16th Article, *Journal des Mathématiques*, ser. 2, vol. 9, 1864, pp. 389–400. Since both this paraphrase and that first given are equivalent to the original theta identity, it must be possible to transform either into the other by elementary means, but I shall not attempt to do so. Both express abstractly identical arithmetical relations.

The substance of Liouville's 13th, 14th and 15th articles (loc. cit. pp. 249–256, 281–8, 321–336), is given in the following paraphrase concerning the same F for the partition (m constant)

$$m = m_1^2 + 4m_2^2 + 2^{\alpha_3+1} d_3\delta_3, \quad d_3, \delta_3 > 0, \quad m_1, d_3, \delta_3 \text{ odd},$$

so that m is odd,

$$\sum F(2^{\alpha_3}\delta_3 - 2m_2,\ d_3 + 2m_2 - m_1,\ d_3 + 2m_2 + m_1,\ 2^{\alpha_3}\delta_3 + m_1) = \sum F\left(\frac{\alpha-\beta}{2},\ \alpha - 2s - 1,\ \beta + 2s + 1,\ \frac{\alpha+\beta}{2}\right),$$

the second $\sum$ referring to $s = 0, 1, 2, \cdots, (\alpha - 3)/2$ over all solutions (α, β) of $2m = \alpha^2 + \beta^2$ (so that α, β are necessarily both odd) in which $\alpha > 1$ and β has the sign that makes $(\alpha + \beta)/2$ odd. (See for fuller details Liouville, loc. cit., pp. 321–336). This is one paraphrase of the easily proved fact (which follows without difficulty from Jacobi's identities) that

$$[\psi(w, z, u) - \psi(w, -z, -u)]\,\vartheta_2(v - z, q^2)\,\vartheta_1(v),$$

in which

$$\psi(w, z, u) = \vartheta_0\left(\frac{w+z+2u}{2}\right)\vartheta_3(w-u, q^2)\,\vartheta_0\left(\frac{w-z}{2}\right),$$

is unchanged in value when u, v, z are replaced by $v, u, -z$ respectively. For, from this we infer at once

$$\begin{aligned}
&\varphi_{001}\left(\frac{w+z}{2}, \quad u\right)\vartheta_2(v-z, q^2)\,\vartheta_3(w-u, q^2)\\
+\,&\varphi_{001}\left(\frac{w-z}{2}, -u\right)\vartheta_2(v-z, q^2)\,\vartheta_3(w+u, q^2)\\
-\,&\varphi_{001}\left(\frac{w-z}{2}, \quad v\right)\vartheta_2(u+z, q^2)\,\vartheta_3(w-v, q_2)\\
-\,&\varphi_{001}\left(\frac{w+z}{2}, -v\right)\vartheta_2(u+z, q^2)\,\vartheta_3(w+v, q^2) = 0,
\end{aligned}$$

an identity in w, z, u, v which paraphrases immediately into the stated theorem on substituting the expansions and proceeding as before. By means of the transformation of the second order either of these φ identities can be inferred from the other, but it is simpler to deduce them separately from Jacobi's lists of theta formulas.

Another of Liouville's theorems of a similar kind for which no proof has been published is the following, which he used in obtaining several of his class number relations. The odd constant integer $m > 0$ is partitioned as follows,

$$m = 2m'^2 + d''\delta'', \qquad 2m = m_1^2 d_2 \delta_2,$$

in which d'', δ'', d_2, $\delta_2 > 0$ are odd, m_1 is odd, and these are all the restrictions on the integer variables. Then it is stated that (loc, cit., vol. 7, p. 42),

$$\begin{aligned}
2\sum F(d''+2m',\ \delta''-2m',\ 2m'+d''-\delta'')\\
= \sum F\left(\frac{d_2+\delta_2}{2},\ m_1,\ \frac{d_2-\delta_2}{2}\right),
\end{aligned}$$

where $F(x, y, z) = f((y, z)\,|\,x)$, this f being an unrestricted parity function of the parity indicated. The theorem is the

paraphrase of an immediate consequence of the following special case of one of Jacobi's identities.

$$\begin{aligned}\vartheta_2\vartheta_1(b+c)\vartheta_3(c+a)\vartheta_0(a+b)\\ = \vartheta_3(a+b+c)\vartheta_0(a)\vartheta_2(b)\vartheta_1(c)\\ +\vartheta_0(a+b+c)\vartheta_3(a)\vartheta_1(b)\vartheta_2(c).\end{aligned}$$

Change the signs of b, c. Then, by elimination,

$$\begin{aligned}\vartheta_2\vartheta_3(c-a)[\vartheta_1(b+c)\vartheta_0(b-a)\vartheta_3(b-c-a)\\ +\vartheta_1(b-c)\vartheta_0(b-a)\vartheta_3(b+c-a)]\\ = \vartheta_3(a)\vartheta_1(b)\vartheta_2(c)[\vartheta_3(b+c-a)\vartheta_0(b-c+a)\\ +\vartheta_0(b+c-a)\vartheta_3(b-c+a)].\end{aligned}$$

Factoring the last by the addition theorems for the thetas we find finally

$$\begin{aligned}\vartheta_1'[\vartheta_1(b+c)\vartheta_0(b-a)\vartheta_3(b-c+a)\\ +\vartheta_1(b-c)\vartheta_0(b-a)\vartheta_3(b+c-a)]\\ = 2\vartheta_0(b)\vartheta_1(b)\vartheta_3(b)\vartheta_2(c)\vartheta_3(a)\vartheta_0(c-a).\end{aligned}$$

By means of the last identity we readily see that

$$\begin{aligned}4[\varphi_{100}(x+z,y-z,q^2)\,\vartheta_3(x-y+z,q^2)\\ +\varphi_{100}(x-z,-y+z,q^2)\,\vartheta_3(x+y-z,q^2)]\\ = \vartheta_2(y,q^2)\left[\varphi_{100}\left(\frac{x+z}{2},\frac{x-z}{2}\right)+\varphi_{133}\left(\frac{x-z}{2},\frac{x+z}{2}\right)\right.\\ \left.+\varphi_{100}\left(\frac{x-z}{2},\frac{x+z}{2}\right)+\varphi_{133}\left(\frac{x-z}{2},\frac{x+z}{2}\right)\right].\end{aligned}$$

Using the expansions of φ_{100}, φ_{133} as given in the papers cited in § 12 we have the theorem.

This example illustrates a useful algorithm. Starting from any of Jacobi's (or Briot and Bouquet's) theta identities, we change the signs of one or more variables and eliminate terms unchanged or changed only in sign by these transformations. We then use the addition theorems for the thetas to separate sums into products, or inversely. Last, by the

transformation of the second order we can frequently reduce the number of theta factors in several of the products before division of the entire identity by the same theta product to introduce functions of the second kind. There is no difficulty in writing down $\vartheta.\ \varphi$ identities concerning products of many factors. The desideratum, to reach simple paraphrases, is that the number of factors $\vartheta.\ \varphi$ in each term of an identity deduced from a given identity shall be a minimum. This is the origin of the several reductions in the above examples. Any stage of the reduction yields a paraphrase; all such are arithmetically equivalent, although this may be troublesome to prove by elementary methods in a given instance.

Continuing with the examples we find from Jacobi as just indicated that

$$\begin{aligned}&[\vartheta_0(x+u)\ \vartheta_1(x+u)\ \vartheta_0(x-u+v)\ \vartheta_1(x-u+v)\ \vartheta_3(x-2v)\\ &-\vartheta_0(x-u)\ \vartheta_1(x-u)\ \vartheta_0(x+u-v)\ \vartheta_1(x+u-v)\ \vartheta_3(x+2v)]\\ &\qquad\times\vartheta_0(u)\ \vartheta_1(u)\end{aligned}$$

is invariant when u, v are interchanged. Putting $u=y+z$, $v=y-z$ we get after a few simple reductions

$$\begin{aligned}&\varphi_{111}\left(\frac{x+2z}{2},\ \frac{y-z}{2},\ q^{1/2}\right)\ \vartheta_3\left(\frac{x-2y+2z}{2}\right)\\ &+\varphi_{111}\left(\frac{x-2z}{2},\ \frac{-y+z}{2},\ q^{1/2}\right)\ \vartheta_3\left(\frac{x+2y-2z}{2}\right)\\ &-\varphi_{111}\left(\frac{x-2z}{2},\ \frac{y+z}{2},\ q^{1/2}\right)\ \vartheta_3\left(\frac{x-2y-2z}{2}\right)\\ &-\varphi_{111}\left(\frac{x+2z}{2},\ \frac{-y-z}{2},\ q^{1/2}\right)\ \vartheta_3\left(\frac{x+2y+2z}{2}\right)=0,\end{aligned}$$

an identity in x, y, z, which paraphrases at once into

$$\begin{aligned}&\sum F(\delta''+m',\ \delta''-2m',\ 2\delta''+2m'-\delta'')\\ &\qquad=\varepsilon(m)\left[\sum_s F(m^{1/2},\ s,\ s)-\sum_t F(t,\ 2m^{1/2},\ 2t)\right],\end{aligned}$$

where F is the parity function

$$F(x, y, z)\equiv f(x, y, z);$$

the $\sum$ on the left refers to the partition

$$m = m'^2 + d''\,\delta'', \qquad m' \geqq 0, \qquad d'', \qquad \delta'' > 0,$$

for m fixed (the integers m, m' d'', δ'' are without further restrictions); $\varepsilon(m) = 1, 0$ according as m is or is not a square; $\sum_s$, $\sum_t$ refer respectively to

$$s = 1, 2, \cdots, 2m^{1/2} - 1, \qquad t = 1, 2, \cdots, m^{1/2} - 1.$$

This is the substance of Liouville's 12th Article, loc. cit. vol. 5 (1860), pp. 1–8.

Completely arbitrary single valued functions of integers (not restricted as to parity) of one or more variables can easily be obtained by the same means as above. But it is to be noticed that, so far as general formulas are concerned (those containing the arbitrary functions), this is no essential gain in generality over the parity paraphrases. When we come presently to the theta functions of $n > 1$ variables we shall see that the arithmetical equivalents of theta identities always involve completely arbitrary functions. One example for the elliptic thetas will suffice. The pseudo-generality is attained by the device of adding an identically vanishing sum to a parity identity.

The expansion of $\vartheta_1'/\vartheta_0(u)$ in the reduced form is given in the papers cited in § 12,

$$\vartheta_1'/\vartheta_0(u) = 2\sum q^{m/4}\left[\sum(-1\,|\,\delta)\cos\left(\frac{d-\delta}{2}\right)u\right],$$

the outer $\sum$ referring to $m = 1, 5, 9, 13, \cdots$, the inner to all $d, \delta > 0$ such that $m = d\delta$. Hence the identity

$$\vartheta_0(u/2)\cdot\vartheta_1'/\vartheta_0(u/2) = \vartheta_1'$$

paraphrases into

$$\sum(-1)^{\nu_1}(-1\,|\,\delta_2) f\left(\nu_1 + \frac{d_2 - \delta_2}{2}\,|\right) = \varepsilon(m)(-1\,|\,m^{1/2})\, m^{1/2} f(0\,|),$$

where $m \equiv 1 \bmod 4$ is constant, and $m = 4\nu_1^2 + d_2\,\delta_2$, $\nu_1 \geqq 0$, $d_2, \delta_2 > 0$. Now, for suitably chosen $f(x\,|)$, $f(|\,x)$

the arbitrary $\varphi(x) \equiv f(x|) + f(|x)$. Hence if it can be shown that over the same partition

$$(A) \qquad \sum (-1)^{\nu_1} (-1|\delta_2) f\left(|\nu_1 + \frac{d_2' - \delta_2}{2}\right) = 0,$$

we shall have proved that

$$\sum (-1)^{\nu_1} (-1|\delta_2) \varphi\left(\nu_1 + \frac{d_2 - \delta_2}{2}\right) = \varepsilon(m)(-1|m^{1/2})\, m^{1/2}\, \varphi(0).$$

By the principle of paraphrase it evidently suffices to prove (A) when $f(|x) \equiv \sin xt$. Expanding $\sin\left(\nu_1 + \frac{d_2 - \delta_2}{2}\right) t$ by the addition theorem we see that it is sufficient to prove, for a particular ν_1, that (t is a parameter)

$$\sum (-1|\delta_2) \sin\left(\frac{d_2 - \delta_2}{2}\right) t = 0.$$

But this is obvious, since to a given term in the sum corresponds a term with d_2, δ_2 interchanged and, for $m \equiv 1 \bmod 4$, $d_2 \delta_2 \equiv 1 \bmod 4$, whence $(-1|d_2) = (-1|\delta_2)$. Thus the φ identity is proved. This was stated by Liouville, 11th Article, loc. cit. vol. 4 (1859), pp. 281–304. The other main formula (π) of this Article is the paraphrase of an equally obvious theta identity. Expressing

$$\vartheta_2(x+2y)\,\vartheta_3(x-2y) + \vartheta_2(x-2y)\,\vartheta_3(x+2y)$$

as a product, multiplying both sides of the resulting identity by $\vartheta_1'\,\vartheta_0(y, q^{1/2})\,\vartheta_3(y, q^{1/2})$ and dividing out by $\vartheta_3(x)\,\vartheta_0(2y)$, we get

$$[2\varphi_{230}(x, 2y)\,\vartheta_3(2y-x) + \varphi_{230}(x, -2y)\,\vartheta_3(2y+x)]$$
$$= \varphi_{230}(y, y, q^{1/2})\,\vartheta_2(x) + \varphi_{230}(-y, -y, q^{1/2})\,\vartheta_2(x),$$

which gives Liouvilles's (π) as stated (the explicit form will be found in Dickson's History, loc. cit.).

These examples will suffice to show that even trivial theta identities yield interesting results. We have chosen known theorems as illustrations to suggest the ready means of proving

or disproving any such formula which may have been stated. Moreover from the theta identity giving the algebraic proof an indefinite number of further theta identities can be constructed by multiplications, resolutions into factors, eliminations, etc., from which additional paraphrases can be obtained. We give no examples of the specific arithmetical theorems which such parity identities imply upon specializing the parity functions, as we are concerned primarily with general methods.

If no shorter way of tracing the theta origin of a parity theorem suggests itself the following will always lead to the equivalent identity between theta quotients. Replace the given theorem (3.12) (3.22) by its special case (3.11)–(3.31). Separate all trigonometric products into sums. Rearrange the arguments in these sums as linear functions with respect to the x, y variables. By inspection it is then easy to write down the product of thetas and φ's (or theta quotients) which generate these terms, on glancing also at the partitions involved. The resulting theta identity is then to be proved from first principles by means of the classical relations between the functions. The reverse process is of course the natural one—start from theta identities and deduce paraphrases. In all such work full lists of theta expansions are necessary.

16. Application to class number relations. We take space to indicate only two of the methods by which paraphrases lead to class number relations. The first was pointed out by Liouville, see H. J. S. Smith, *Report on the Theory of Numbers*, Art. 136, or Dickson's *History*, vol. 3, chapter VI. It consists in choosing for $f(x)$ in a given paraphrase arising from a cosine identity its instance $\varphi(x)$, where $\varphi(x) = 1$ or 0 according as $|x| = c$ or $|x| > c$. This leads to identities concerning numbers of representations in quadratic (binary) forms; at least one enumerative function thus encountered will in general involve one or other of the class number functions F, F_1 or a linear combination of them, $F + F_1 = G$, etc.

The second method applies those arithmetical expansions for theta quotients which directly involve F, F_1, G, $\cdots$. The derivation of such expansions ultimately depends upon the

classical theory of binary quadratic forms. Examples of the last will be found in Humbert's memoir cited in § 12. Assuming that we possess several such expansions we can apply processes similar to those of § 15 to deduce an indefinite number of paraphrases. These will involve the class number functions and parity functions. By specializing the latter we obtain any desired number of class number relations. Both methods can be used with profit simultaneously. An application of the first method to a given paraphrase suggests reductions in obtaining expansions useful for the second. A fruitful special case of $f(x|)$ in these connections is $f(x) = 1$ or 0 according as $x \equiv 0 \bmod m$ is true of false.

An extremely prolific identity for class number relations is the following, due to Professor J. Ouspensky (references will be given presently), who proves it by elementary means. For the partition

$$m = \nu^2 + d\delta$$

of the arbitrary constant integer $m > 0$, where ν, d, δ are integers, and $\nu \gtrless 0$, d, $\delta > 0$, he shows that

$$\sum [\varphi(d+\delta, \nu, d-\delta) - 2\varphi(\delta - 2\nu, d+\nu, 2d-\delta+2\nu)]$$
$$= \varepsilon(m) \sum [\varphi(2m^{1/2}, m^{1/2}-j, 2m^{1/2}-2j)$$
$$- \varphi(2m^{1/2}-j, m^{1/2}, 2m^{1/2}-j)],$$

where $\varphi(x, y, z)$ is the parity function

$$\varphi(x, y, z) \equiv f((y, z)|x),$$

$\varepsilon(m) = 1$ or 0 according as m is or is not a square, as before, and the sum on the right refers to $j = 1, 2, \cdots, 2m^{1/2}-1$. This formula can also be proved from the identity

$$\begin{vmatrix} a_3 & b_3 & c_3 \\ a_3 & b_3 & c_3 \\ a_2 & b_2 & c_2 \end{vmatrix} = 0,$$

on taking

$$a_j = \vartheta_j(2x+y+2z), \quad b_j = \vartheta_j(2x-y-2z),$$
$$c_j = \vartheta_j(y) \qquad (j = 2, 3);$$

whence

$$\varphi_{111}(x+z,\ x-z,\ q^{1/2})\,\vartheta_3(y) = \varphi_{111}(x-z,\ y+2z,\ q^{1/2})\,\vartheta_3(2x-y-2z) + \varphi_{111}(x+z,\ -y-2z,\ q^{1/2})\,\vartheta_3(2x+y+2z),$$

from which the theorem follows at once by paraphrasing.

The fundamental character of the φ formula is amply demonstrated by Professor Ouspensky's applications. Leaving class numbers for a moment, we may call attention to one of these in another direction. An instance of $\varphi(x, y, z)$ is clearly $(-1\,|\,z)\ (-1)^y\ \psi(y, x)$ where $\psi(y, x)$ is the parity function $f(y, x)$, provided z be an odd integer. It is readily seen that the φ identity gives for this choice the following,

$$\sum(-1\,|\,\delta)\,\psi(d+\nu, \delta-2\nu) = \varepsilon(m)(-1)^{m^{1/2}-1}\sum(-1\,|\,j)\,\psi(m^{1/2}, j),$$

where δ is now restricted to be odd. By choosing for ψ its instance $\psi(x, y) = xy$, the classical theorem concerning the number of representations of m as a sum of 2 squares is obtained; similarly from $\psi(x, y) = x^3y$ and $\psi(x, y) = xy^3$ the like for 6 squares follows; for 10 squares there are three such choices, x^5y, x^3y^3, xy^5, and so on. For 4, 8, 12, ... squares we start from other immediate consequences of the fundamental formula, and by equally simple specializations obtain the numbers of representations. The application in all cases proceeds from the following easily proved lemma, (*Bulletin de l'Académie des Sciences de l'URSS*, 1925, pp. 647–662, where the proofs of the theorems indicated above are given in detail). *Let $N_p(m)$ = the number of representations of m by a sum of p squares, and let $\Phi(m)$ denote an arithmetical function defined for $m = 0, 1, 2, \cdots$. Then, if $\Phi(0) = 1$, and*

$$\sum\nolimits_\nu[m-(p+1)\nu^2]\,\Phi(m-\nu^2) = 0, \qquad \nu = 0, \pm1, \pm2, \cdots,$$

the sum continuing so long as $m-\nu^2 \geqq 0$, this implies $N_p(m) = \Phi(m)$. We thus have a new approach to the problem of enumeration of representations as sums of squares.

Returning to class numbers, we can only indicate the power of Professor Ouspensky's identity by stating a few of his applications. First, by easy specializations of φ and combination of the results he deduces a number of related general formulas, all of importance in class number relations. It is an interesting exercise to follow the evolution of these identities (and other of a similar kind) from elementary algebraic transformations of the equivalent theta identity which generates the general formula. The author then determines (by the method first used by Hermite in proving Kronecker's class number relations, indicated at the beginning of this section) the numbers of solutions of certain indeterminate equations of the second degree when the indeterminates are linearly restricted, for example

$$4n+1 = d\delta+2d'\delta',$$

where d, δ, d', δ' are integers >0, $2d' = d+\delta\pm 2$, and δ is odd. In the algebraic method such results are most easily reached by taking $f(x|) \equiv 1$ or 0 according as $|x| = c$ or $|x \neq c$, where $c \geqq 0$ is a constant integer, in the simplest paraphrases deduced from Humbert's expansions. Among the class number formulas which the author proves by these strictly elementary methods are the classical eight of Kronecker, those of grade 2 of Stieltjes, and those of grade 5 of Petr. A class number relation is said to be of grade k if in it the arguments of the class number functions decrease by integers of the form kh^2, where the several h are in arithmetical progression. The first derivations of such relations were by applications of the whole machinery of the elliptic modular functions; here they are referred to elementary arithmetic. Similar derivations are given of relations of the Hurwitz and Humbert types, and those of grade 3 of Petr, also of Liouville's. Finally the relations of grade 5 due to Gierster and Chapelon are obtained, and the method is capable of indefinite extension. Incidentally many new relations are indicated in the course of the derivations. These memoirs are a striking example

of the great richness of paraphrases obtainable from the elements of elliptic theta quotients. They are published in the *Bulletin de l'Académie des Sciences de l'URSS.* 1925 6, in six memoirs.

To illustrate the second method of deducing class number relations from paraphrases we take the identity

$$\vartheta_2^2\vartheta_3\vartheta_1^2(x)\,\vartheta_2(x)\,\vartheta_0^2(x) = [\vartheta_2\vartheta_3\vartheta_1(x)\,\vartheta_0(x)]\cdot[\vartheta_2\vartheta_1(x)\vartheta_2(x)/\vartheta_0(x)],$$

the function on the left being that whose expansion introduces the class number functions. For if as usual $F(n)$ denotes the number of odd classes of binary quadratic forms of negative determinant $-n$, we have for the expansion of the theta quotient on the left

$$2\sum q^{\alpha+4}\left[2\sum F(\alpha-b^2)\cos bx - \sum'(\delta-d)\cos\left(\frac{\delta+d}{2}\right)x\right],$$

where the first $\sum$ extends to $\alpha = 1, 5, 9, 13, \cdots$, the second to all odd integers $b \gtrless 0$ such that $\alpha - b^2 \geq 0$, and $\sum'$ to all pairs (δ, d) of divisors >0 of α such that $d<\delta$. The expansion of the first theta quotient on the right is

$$4\sum q^{m^2}\left(\sum \sin \tau x\right) \qquad (m = 1, 3, 5, \cdots;\ m = t\tau,\ \tau > 0);$$

that of the second is

$$4\sum q^{\beta/4}\left[\sum' \sin\left(\frac{\delta+d}{2}\right)x\right], \qquad (\beta = 3, 7, 11, 15, \cdots),$$

where $\sum'$ refers to those divisors δ, $d>0$ of β such that $\beta = d\delta$, $d<\delta$. The paraphrase is therefore

$$2\sum F(\alpha-b^2)f(b) = \sum'(\delta-d)f\left(\frac{\delta+d}{2}\right) + 2\sum\left[f\left(\frac{\delta_2+d_2}{2}-\tau_1\right)-f\left(\frac{\delta_2+d_2}{2}+\tau_1\right)\right],$$

the $\sum$ on the left referring to b as above, and those on the right to all positive integers defined by

$$\alpha = 2m_1+\beta_2,\quad \alpha = d\delta,\quad d<\delta,\quad m_1 = t_1\tau_1,\quad \beta_2 = d_2\delta_2,$$

where the constant integer $\alpha \equiv 1 \bmod 4$, and $\beta_2 \equiv 3 \bmod 4$, all d, δ, δ_2, d_2, τ_1 (the last necessarily odd) satisfying these conditions being taken; $f(x) \equiv$ the parity function $f(x)$. By specializing $f(x)$ an infinity of class number relations are obtainable, and all these are equivalent to the given theta identity. The applications of the parity considerations regarding forms in §§ 6—11 are particularly interesting, but we need not stop to write out examples, several of which are given elsewhere.

Paraphrases involving functions of order ω may be called ω-fold infinite, for an obvious reason. The above example is a singly infinite class number relation. It is not difficult to obtain ω-fold infinite class number relations for $\omega = 1, 2, 3, 4$ from Humbert's expansions and Jacobi's formulas. From all the examples given the general significance of the orders and degrees ω, ω_0, ω_1, δ, δ_0, δ_1 of parity functions in § 3 and its relation to the theta quotients giving rise to the respective paraphrases is evident.

APPLICATION TO THETA FUNCTIONS OF $p>1$ ARGUMENTS, §§ 17-20

17. Arithmetical expansions of the theta functions of $p>1$ arguments. In one of the customary notations for these functions we have the expansion (for conditions of convergency see Krazer, *Lehrbuch der Thetafunktionen*, or Harkness and Morley, *Theory of Functions*),

$$\vartheta\begin{bmatrix} g \\ h \end{bmatrix}^{(v)} \equiv \begin{bmatrix} g_1\, g_2 \cdots g_p \\ h_1\, h_2 \cdots h_p \end{bmatrix}^{v_1, v_2, \cdots, v_p}$$

$$= \sum_{n_1, \cdots, n_p}^{-\infty, \infty} \exp\ \pi i \left[\sum_{r=1}^{p} \sum_{s=1}^{p} \tau_{rs} (n_r + \frac{1}{2} g_r)(n_s + \frac{1}{2} g_s) + 2 \sum_{r=1}^{p} (n_r + \frac{1}{2} g_r)(v_r + \frac{1}{2} h_r) \right],$$

with $\tau_{rs} = \tau_{sr}$, and each of g_j, h_j a definite one of 0,1.

Define ν_r, u_r, q_r, $\cdots$, by

$$2n_r + g_r = \nu_r, \quad \pi v_r = u_r, \quad \exp(i\pi\tau_{rr}/4) = q_r \ (r = 1, \cdots, p),$$

$$[h\nu] = \exp\left(\frac{\pi i}{2}\sum_{j=1}^{p} h_j \nu_j\right),$$

$$\pi\tau_{r,r+s} = 2u_{r,r+s} \ (r = 1, 2, \cdots, p-1; \ s = 1, 2, \cdots, p-r).$$

Then $[h\nu] = 0, i, -1, -i$ according as $\sum h_j\nu_j \equiv 0, 1, 2, 3 \bmod 4$. The above expansion becomes

$$\sum\left\{[h\nu]q_1^{\nu_1^2}q_2^{\nu_2^2}\cdots q_p^{\nu_p^2}\exp i\left(\sum_{r=1}^{p}\nu_r u_r + \sum_{r=1}^{p-1}\sum_{s=1}^{p-r}\nu_r\nu_s u_{r,r+s}\right)\right\},$$

the $\sum$ referring to $n_r = -\infty$ to ∞ $(r = 1, \cdots, p)$. The ν's in this are integers, the u's independent variables, the q's parameters. This is the form of the expansions required in arithmetic.

We shall require the following lemma, which is proved immediately on separating first reals and imaginaries and observing that in a trigonometric identity involving trigonometric products of different parities all those terms having a given parity may be considered independently of the rest in paraphrasing, and finally recombining terms in an obvious way. *If ξ, z are matric variables of order n, and ξ_j $(j = 1, \cdots, t)$ are t integral values of ξ, then if*

$$\sum_{j=1}^{t} a_j \exp[i(\xi_j z)] = 0 \tag{17.1}$$

is an identity in z, where the a_j are rational numbers or complex numbers of the form $b_j + ic_j$, where b_j, c_j are rational numbers, the identity implies

$$\sum_j a_j \cos(\xi_j z) = 0, \ \sum_j a_j \sin(\xi_j z) = 0,$$

and hence it implies

$$\sum_j a_j f(\xi_j) = 0, \tag{17.2}$$

where $f(z)$ takes a single definite value for all integral values of the matric variable z of order n, and otherwise is entirely arbitrary. Thus identities of the form (17.1) lead to arith-

metical theorems concerning functions wholly arbitrary except as to uniformity for all sets of integral values of their n independent variables.

18. Quasi even and odd arithmetical functions. When several $[h\nu]$ are considered simultaneously we write

$$[h_r\nu_r] \equiv [h_{1r}\nu_{1r},\ h_{2r}\nu_{2r},\ \cdots,\ h_{pr}\nu_{pr}] \equiv \sum_{j=1}^{p} h_{jr}\nu_{jr},$$

and the value of $[h_r\nu_r]$ is $1, i, -1, -i$ according as the sum just written is $\equiv 0, 1, 2, 3 \bmod 4$. In what follows each of

$$g_{jr},\ h_{jr} \quad (j = 1, \cdots, p;\ r = 1, 2, 3, \cdots, 2^{2p})$$

denotes a definite one of 0, 1; each n_{jr} is an integer (positive, zero or negative); $\nu_{jr} = 2n_{jr} + g_{jr}$. The $[h_r\nu_r]$ are multiplied according to

$$[h_r\nu_r]\,[h_s\nu_s] = [h_{1r}\nu_{1r} + h_{1s}\nu_{1s},\ h_{2r}\nu_{2r} + h_{2s}\nu_{2s},\ \cdots,\ h_{pr}\nu_{pr} + h_{ps}\nu_{ps}].$$

The *characteristic*

$$\begin{bmatrix} g_r \\ h_r \end{bmatrix} \equiv \begin{bmatrix} g_{1r}\ g_{2r} \cdots g_{pr} \\ h_{1r}\ h_{2r} \cdots h_{pr} \end{bmatrix} \tag{18.1}$$

is called *even* or *odd* according as $\sum_{j=1}^{p} g_{jr}h_{jr}$ is even or odd.

From the ν_{jr} $(j = 1, \cdots, p)$ and their products $\nu_{jr}\,\nu_{kr}$ $(j, k = 1, \cdots, p, j \neq k)$ we construct the function

$$[h_r\nu_r]\,L(\nu_{1r}, \nu_{2r}, \cdots, \nu_{pr},\ \nu_{1r}\nu_{2r}, \cdots, \nu_{1r}\nu_{pr},\ \nu_{2r}\nu_{3r}, \cdots, \nu_{p-1,r}\nu_{pr})$$

where L is a function of $p(p+1)\ 2$ arguments which takes a single definite value for each set of integral values of all its arguments, and which otherwise is arbitrary. The product $[h_r\nu_r]\,L(\ )$ just written will be abbreviated to either of the forms

$$l\begin{bmatrix} g_r \\ h_r \end{bmatrix}^{(\nu_r)}, \qquad l(\nu_r) \tag{18.2}$$

as convenient. This function has by definition the *characteristic* (18.1) and $l(\nu_r)$ is called *quasi even* or *quasi odd* according as its characteristic is even or odd. The function obtained

from a quasi even $l(\nu_r)$ on replacing each of the first p arguments in L by zero is denoted by either of

$$\lambda \begin{bmatrix} g_r \\ h_r \end{bmatrix}^{(\nu_r)}, \qquad \lambda(\nu_r) \tag{18.3}$$

and is called a *quasi constant*. By the usual theory of theta characteristics (which can be transposed verbatim to these functions) we see that there are precisely $2^{p-1}(2^p+1)$ quasi even $l(\nu_r)$, and hence the same number of quasi constants, and $2^{p-1}(2^p-1)$ odd $l(\nu_r)$. The paraphrase of identities between thetas in p arguments leads to arithmetical theorems concerning functions (18.2), (18.3) for sets of integral values of the arguments obtained from the simultaneous solutions of a set of indeterminate equations.

19. **Products** l, λ. The paraphrases refer to certain products, in a technical sense, next defined. Let $t \geqq 1$, $\tau \geqq 0$ be constant integers, and $n_r\,(r=1,\cdots,p)$ arbitrary constant integers >0. For the ν_{rj} as already defined consider the set of all (integral) solutions ν_{rj} of the p equations

$$n_r = \sum_{j=1}^{t+\tau} \nu_{rj}^2 \qquad (r=1,\cdots,p). \tag{19.1}$$

Set

$$[h] \equiv \prod_{j=1}^{t+\tau} [h_j\,\nu_j], \qquad \alpha_r \equiv \sum_{j=1}^{t} \nu_{jr} \qquad (r=1,2,\cdots,p),$$

$$\beta_{r,r+s} \equiv \sum_{j=1}^{t+\tau} \nu_{rj}\,\nu_{r+s,j} \quad (r=1,\cdots,p-1;\ s=1,2,\cdots,p-r),$$

and for each solution of the system (19.1) construct the function

$$[h]\,L(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_p,\ \beta_{12},\ \beta_{13},\ \cdots,\ \beta_{1p},\ \beta_{23},\ \cdots,\ \beta_{2p},\ \cdots,\ \beta_{p-1,p}).$$

Take the sum of all values of the last over all (necessarily finite in number) solutions of (19.1) and denote it by

$$(n_r)\,|\,l(\nu_1)l(\nu_2)\cdots l(\nu_t)\lambda(\nu_{t+1})\lambda(\nu_{t+2})\cdots\lambda(\nu_{t+\tau}).$$

We call this the l, λ product, or simply the product of

$$l(\nu_j),\ \lambda(\nu_k) \qquad (j=1,\cdots,t;\ k=t+1,\cdots,t+\tau).$$

Such multiplication is commutative. If the parameters $(n_r) \equiv (n_1, n_2, \cdots, n_p)$ are understood we omit the (n_r)| and write

$$\mathcal{A}(v) \equiv l(v_1) \cdots l(v_t)\lambda(v_{t+1}) \cdots \lambda(v_{t+\tau}).$$

If $\tau = 0$ the factors λ are absent. Clearly $\mathcal{A}(v)$ is uniquely determined by (n_r) and the characteristics

$$\begin{bmatrix} g_r \\ h_r \end{bmatrix}, \begin{bmatrix} g_s \\ h_s \end{bmatrix} \qquad (r = 1, \cdots, t;\ s = t+1, \cdots, \tau)$$

of the $l(v_r)$, $\lambda(v_s)$ respectively. Hence if preferred $\mathcal{A}(v)$ may be considered as a function of (n_r) and these characteristics.

In determining the degree of a product $\mathcal{A}(v)$ we treat the quasi constants as absolute constants. The *degree* of $\mathcal{A}(v)$ as above is therefore t. Hence a linear homogeneous relation between products of degree t is defined.

20. Abstract identity of the theory of the p fold thetas and that of l, λ products. Let

$$\sum_{j=0}^{n} k_j \mathcal{A}_j(v) \tag{20.1}$$

be a homogeneous linear relation between products of degree t, and let the characteristics of the l, λ in $\mathcal{A}_j$ be

$$\begin{bmatrix} g_r^{(j)} \\ h_r^{(j)} \end{bmatrix} \qquad (r = 1, 2, \cdots, t;\ j = 0, 1, \cdots, n). \tag{20.2}$$

Consider the theta functions of p arguments v_r having the characteristics (20.2) and in the last τ of these put $v_r = 0$ $(r = 1, \cdots, p)$. Denote the (common algebraic) product of the t theta functions and τ theta constants thus obtained by $\Theta_j(v)$. Then (20.1) *implies*

$$\sum_{j=0}^{n} k_j \Theta_j(v) = 0, \tag{20.3}$$

and conversely, (20.3) *implies* (20.1).

For, from preceding sections, it is easily seen that the result of equating to zero the coefficient of $q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r}$ in (20.3) is the special case of (20.1) in which each function L

is replaced by the exponential function of $i\,(=(-1)^{1/2})$ times the scalar product of the argument of L and the matrix of order $p(p+1)/2$ whose elements are v's, u's in § 17. By the lemma in § 17 the converse above stated follows; from the converse follows the exponential form of the theorem and thence, by multiplying by $q_1^{n_1}\, q_2^{n_2} \cdots q_r^{n_r}$ and summing with respect to $n_1, n_2, \cdots, n_r$ we get (20.3).

Hence *in any identity between theta products* (such as, for example, the classical biquadratic relations) *the theta products may be replaced by l, λ products having the same respective characteristics as the thetas, all such products being taken over the same* (n_r).

Thus the algebraic part of the theory of the thetas is equivalent to sets of identities between arbitrary single valued functions of integers satisfying sets of indeterminate equations of the second degree. The pseudo periodicity can easily be traced to the transformations which such identities undergo when the numbers of odd, even variable integers in the sets of equations are changed. By means of the parity forms developed in §§ 6-11 the set of indeterminate equations of the *second* degree can be replaced by equations of *arbitrary* degrees, or such extensions can be reached directly by imposing on the arbitrary functions in (20.1) the condition that they shall vanish except when one or more of their arguments are integers representable in any preassigned forms, and similarly for other arithmetical restrictions, as, for example, that the functions shall vanish for integral arguments that are residues of assigned powers. This does not of course permit us to replace (19.1) by a set of conditions given at random; the manner in which (19.1) still dominates (20.1) even when (19.1) is replaced by a set of equations of degree ≥ 2 will be evident on working through any special case, say that of the thetas of 2 arguments.

CHAPTER IV

APPLICATIONS OF THE ALGEBRAS $\mathfrak{C}$, $\mathfrak{D}$

ALGEBRA $\mathfrak{E}$, §§ 1–9

1. Scope of *E*. What follows is a short introduction to an extensive branch of algebraic arithmetic, namely to its multiplicative aspect. In this the algebra $\mathfrak{E}$, a species of resultant of $\mathfrak{C}$, $\mathfrak{D}$, plays the central part; $\mathfrak{E}$ is an algebra of unique multiplicative decomposition. The basic concept is that of composition of matrices. Although addition and subtraction are defined in $\mathfrak{E}$, and are abstractly identical with the like in $\mathfrak{A}$, they are of less interest than multiplication and division, and their detailed development may be omitted. Multiplication and division in $\mathfrak{E}$ will be placed in (1,1) correspondence with the multiplicative properties of functions of two independent variables in $\mathfrak{A}$. From relations between such functions we infer without computations relations between functions of any elements for which unique factorization subsists. When the functions in $\mathfrak{A}$ are restricted to be rational and integral, the correspondence gives an arithmetic in $\mathfrak{E}$ abstractly identical with rational arithmetic. As $\mathfrak{E}$ or its special arithmetic has great power over the algebra of the great mass of existing arithmetical functions, and as it is also extremely effective in devising new functions and classifying their algebraic properties, we shall state its processes in detail. From this several possible generalizations will be apparent, particularly to the properties of sets of functions of elements for which the fundamental theorem of arithmetic holds. The initial treatment is abstract, as $\mathfrak{E}$ has been constructed to include a wide range of existing algebraic relations between arithmetical functions and to make possible indefinite extensions in similar or essentially new directions.

2. Composites. Let $\mu_j (j = 0, 1, \cdots)$ be a set of matrices, finite or infinite in number, each of finite or infinite

order, whose elements belong to a commutative semigroup $\mathfrak{S}$ having a unity. Then if each element of μ_0 is the product in $\mathfrak{S}$ of one and only one element from each of μ_k $(k = 1, 2, \cdots)$, μ_0 is called a *composite* of $\mu_1, \mu_2, \cdots$. Such a composite is uniquely determined only when the law of selection of elements from the μ_k to be multiplied together to produce elements of μ_0 is specified. The algebra $\mathfrak{E}$ is defined by such a law when (and only when) all of the matrices μ_j are of infinite order.

The following theory can be generalized at once to any set of elements closed under any operation which generates from any pair of elements of the set a unique element in the set. Composites are then defined with respect to this operation which replaces multiplication in $\mathfrak{S}$. Thus, for example, there is a theory of additive composition of matrices whose elements belong to a module or to a finite field.

3. Primary and derived matrices. Let s be any matrix in $\mathfrak{S}$ of infinite order,

$$s \equiv (s_1, s_2, \cdots) \tag{3.1}$$

whose first element s_1 is the unity in $\mathfrak{S}$, so that $s_1 s_n = s_n$ $(n = 1, 2, \cdots)$. Let p_n be the nth rational prime, 1 being counted the first, $p_1 = 1$, $p_2 = 2$, $p_3 = 3$, $p_4 = 5, \cdots$. In (3.1) make the following change in notation

$$s_j = x_{p_j} \qquad (j = 1, 2, \cdots), \tag{3.2}$$

and write

$$x \equiv (x_1, x_2, x_3, x_5, x_7, x_{11}, x_{13}, x_{17}, \cdots), \tag{3.3}$$

so that $x = s$, and x_k is an element of x only if k is prime. We call x the *primary form* of s. Any matrix in $\mathfrak{S}$ with first element the unity in $\mathfrak{S}$ can be written in primary form. For distinct matrices $s, r, \cdots$ in $\mathfrak{S}$ we may use different new variables $x, y, \cdots$ (with prime suffixes).

Let $a, b, \cdots, c$ be rational integers $\geqq 0$, and let $x_\alpha, x_\beta, \cdots, x_\gamma$ be distinct elements of x in (3.3). Then $\alpha, \beta, \cdots, \gamma$ are

distinct primes $\geqq 1$. If $a = b = \cdots = c = 0$ we define $x_\alpha^a x_\beta^b \cdots x_\gamma^c$ to be the unity in $\mathfrak{S}$, so that the value of this product is $s_1 = x_1$. Let each of $a, b, \cdots, c$ be now a rational integer > 0, and $\alpha, \beta, \cdots, \gamma$ distinct primes > 1, and let

$$n = \alpha^a \beta^b \cdots \gamma^c \tag{3.4}$$

be the resolution of $n > 1$ into powers of distinct primes > 1. Then we define the element x_n of $\mathfrak{S}$ by

$$x_n \equiv x_\alpha^a x_\beta^b \cdots x_\gamma^c, \qquad x_1 = s_1. \tag{3.5}$$

Hence $x_m (m \geqq 1)$ is a uniquely defined element of $\mathfrak{S}$, and the D matrix

$$x' \equiv (x_1, x_2, x_3, x_4, \cdots, x_n, \cdots) \tag{3.6}$$

in $\mathfrak{S}$ has as elements all products in $\mathfrak{S}$ of positive integral powers in $\mathfrak{S}$ of elements of the original s in (3.1); moreover the first element of x' is the unity in $\mathfrak{S}$, and x' is a uniform function in $\mathfrak{S}$ of s. We shall call x' in (3.6) the *derived matrix* of the primary x in (3.3).

We have therefore defined in any commutative semigroup $\mathfrak{S}$ having a unity the primary and derived matrices (3.3), (3.6) of any given matrix (3.1) whose first element is the unity in $\mathfrak{S}$. Taking now x' as the given matrix in $\mathfrak{S}$ we can form its primary, and from the latter, by forming the derived matrix, we obtain the second derived matrix x'' of the primay x, and so on indefinitely. In what follows we shall attend only to x, x'.

Addition in $\mathfrak{S}$ is without meaning. We next construct from all the elements of $\mathfrak{S}$ matrices of functions, on the hypothesis that a certain ring of such functions exists.

4. The modified ring $\mathfrak{R}_S$ of $\mathfrak{S}$. A set Σ' of elements is said to form a *modified ring* if (1) Σ' is a ring, and (2) in Σ' there exists an element having with respect to multiplication the properties of unity.

Consider now the set Σ of all primary matrices and their (first) derived matrices in $\mathfrak{S}$. Let w be any one of the

primaries, and let w_α be any element of w, so that $\alpha \geqq 1$ is prime. We shall now assume that *the set of all symbols*

$$f_a(w_\alpha),\ g_a(w_\alpha),\ h_a(w_\alpha), \cdots \qquad (a = 0, 1, \cdots;\ \alpha \text{ prime} \geqq 1)$$

are the elements of a modified ring, $\mathfrak{R}_S$, *in which each of*

$$f_0(w_\alpha),\ g_0(w_\alpha),\ h_0(w_\alpha), \cdots \qquad (\alpha \text{ prime} \geqq 1)$$

denotes the unity, and in which addition, multiplication, and division by the unity, are indicated as in $\mathfrak{A}$. For example $f_a(w_\alpha)\, g_a(w_\alpha)$ denotes the product in $\mathfrak{R}_S$ of $f_a(w_\alpha)$ and $g_a(w_\alpha)$.

Division in $\mathfrak{R}_S$ is defined only (by the above) when the divisor is a product of powers of the unity in $\mathfrak{R}_S$. It is not assumed that multiplication in $\mathfrak{R}_S$ has the same interpretation as in $\mathfrak{S}$; in general the interpretations will be distinct. By the definition of a ring it follows that each of $f_a(w_\alpha), g_a(w_\alpha), \cdots$ is a uniform function of w. We shall refer to the $f_a(w_\alpha)$, $g_a(w_\alpha), \cdots$ as *uniform functions.*

From $\mathfrak{R}_S$ select the set of all uniform functions having as arguments a particular w_δ, say x_δ, where $\delta > 1$ is prime. Arrange these functions in any way into matrices *in each of which the first element is the unity in* $\mathfrak{R}_S$. Without loss of generality we may assume all these now to be C matrices. Let

$$f_\delta \equiv (f_0(x_\delta), f_1(x_\delta), \cdots, f_n(x_\delta), \cdots) \tag{4.1}$$

be any one of them. Then f_δ is called the *primary matrix in* $\mathfrak{R}_S$ *with base* $(f_0, f_1, \cdots, f_n, \cdots)$ *and argument* x_δ. From the definition (see the remarks on functions, chapter I § 8), it follows that f_δ is a uniform function of its argument and base, for when x_δ and the base are assigned, f_δ is uniquely known.

Keeping the base of f_δ fixed and letting δ range over all primes $\alpha, \beta, \gamma, \cdots, \delta, \cdots, > 1$, we obtain the set

$$f_\alpha, f_\beta, f_\gamma, \cdots, f_\delta, \cdots \tag{4.2}$$

of all primary matrices in $\mathfrak{R}_S$ having the given base $(f_0, f_1, \cdots, f_n, \cdots)$.

Each element of f_δ is of the form $f_j(x_\delta)$, where $j \geqq 0$ is an integer and $\delta > 1$ is prime. To define $f_j(x_n)$, where n is either prime or composite, we note that

$$f_a(x_\alpha)\, f_b(x_\beta) \cdots f_c(x_\gamma) \tag{4.3}$$

is in $\mathfrak{R}_S$. With n as in (3.4) we write the uniquely determined element (4.3) of $\mathfrak{R}_S$ in either of the forms $f_x(n)$, $f_n(x)$, so that

$$f_x(n) \equiv f_n(x) \equiv f_a(x_\alpha)\, f_b(x_\beta) \cdots f_c(x_\gamma) \qquad (n > 1), \tag{4.4}$$

and to conform with this we write

$$f_x(1) \equiv f_1(x) \equiv f_0(x_\delta). \tag{4.5}$$

Hence (4.4), (4.5) define $f_x(n) \equiv f_n(x)$ for every integer $n > 0$, and the set of all $f_n(x)$ $(n = 1, 2, \cdots)$ uniquely determines the D matrix

$$f \equiv (f_1(x), f_2(x), \cdots) \equiv (f_x(1), f_x(2), \cdots), \tag{4.6}$$

which we call the *derived matrix in* $\mathfrak{R}_S$ *with the base* $(f_0, f_1, \cdots)$, (see (4.1)), *and the matric argument as in* (3.6).

Algebra $\mathfrak{E}$ is concerned with the laws of combination of derived matrices in $\mathfrak{R}_S$ having the same matric argument x' and any bases. One extension of $\mathfrak{E}$ discusses the like when the arguments are not necessarily the same.

5. ***E* composition.** Consider the elements $f_x(n) \equiv f_n(x)$ of the derived matrix (4.6) and suppose $n > 1$, so that $f_x(n)$ may be taken as in (4.3) with n as in (3.4). Then each of the primaries

$$f_\delta \equiv (f_0(x_\delta), f_1(x_\delta), \cdots) \qquad (\delta = \alpha, \beta, \cdots, \gamma)$$

contributes precisely one factor to $f_x(n)$, the respective factors being $f_a(x_\alpha)$, $f_b(x_\beta)$, $\cdots$, $f_c(x_\gamma)$ and each primary f_ϱ, with ϱ different from each of $\alpha, \beta, \cdots, \gamma$, contributes as

factor to $f_x(n)$ its first element $f_0(x_\varrho)$ only, the last being the unity in $\mathfrak{R}_S$. *Hence f in* (4.6) *is a specific composite,* which we shall call the *E composite, of the set* (4.2) *of all primary matrices in $\mathfrak{R}_S$ having the base* $(f_0, f_1, \cdots, f_n, \cdots)$, and we shall write

$$(5.1) \quad f \equiv (f_1(x), f_2(x), \cdots, f_n(x), \cdots) \equiv E(f_\delta),$$

or in full,

$$(5.2) \quad (f_1(x), f_2(x), \cdots, f_n(x), \cdots) = E(f_0(x_\delta), f_1(x_\delta), \cdots, f_n(x_\delta), \cdots),$$

where δ denotes the particular general prime >1. It may be anticipated that abstractly E composition is a multiplication as δ ranges over all primes >1, and this we shall see is the case. The base, we recall, of the C matrix on the right of (5.2) is $(f_0, f_1, \cdots, f_n, \cdots)$. Let

$$(k_0, k_1, \cdots, k_n, \cdots) \quad (k = f, g, \cdots, h)$$

be a set of bases, not necessarily distinct. Then, as in (5.1), we write the E composites

$$(5.21) \quad f \equiv E(f_\delta), \qquad g \equiv E(g_\delta), \cdots, \qquad h \equiv E(h_\delta),$$

and, as in (4.1), the primaries

$$(5.3) \quad k_\delta \equiv (k_0(x_\delta), k_1(x_\delta), \cdots, k_n(x_\delta), \cdots), \quad (k = f, g, \cdots, h).$$

Take the C product (see chapter I, §§ 17,20) K_δ of all the k_δ in (5.3),

$$(5.4) \quad K_\delta \equiv P_C\{f_\delta, g_\delta, \cdots, h_\delta\} \equiv (K_0(x_\delta), K_1(x_\delta), \cdots),$$

and note that the same argument x_δ occurs in all the factors $f_\delta, g_\delta, \cdots, h_\delta$ of this product. The multiplications and additions by which the elements $K_n(x_\delta)$ $(n = 0,1, \cdots)$ of K_δ in (5.4) are generated from those of (5.3) are in $\mathfrak{R}_S$; the indicated C product P_C in (5.4) is C multiplication with re-

spect to $\mathfrak{R}_S$. The notation K_δ is consistent with what precedes, since each element of the C product is a uniform function in $\mathfrak{R}_S$ with the single argument x_δ, and by the definitions $K_0(x_\delta) =$ the unity in $\mathfrak{R}_S$.

Hence K_δ is a primary matrix in $\mathfrak{R}_S$ and therefore we may form its $\mathfrak{E}$ composite $E(K_\delta)$, say

$$(5.5) \qquad K \equiv E(K_\delta), = E(P_C(f_\delta, g_\delta, \cdots, h_\delta)).$$

Observing now that $f, g, \cdots, h$ by (5.21) are E composites, and noticing by (5.2) that an E composite is a D matrix, we can form the D product of the E composites $f, g, \cdots, h$, say K',

$$(5.6) \quad K' \equiv P_D\{f, g, \cdots, h\} \equiv (K_1'(x), K_2'(x), \cdots).$$

From the definitions now follows at once the extremely useful consequence

$$(5.7) \qquad K' = K,$$

or, indicating the operations more fully, we have

$$(5.8) \quad P_D(E(f_\delta), E(g_\delta), \cdots, E(h_\delta)) = E(P_C(f_\delta, g_\delta, \cdots, h_\delta)).$$

6. The four fundamental operations in $\mathfrak{E}$. We can now summarize $\mathfrak{E}$ in concise form. The *elements* of $\mathfrak{E}$ are all the derived matrices of $\mathfrak{R}_S$ with the same matric argument x' (see (4.6)).

If f, g are any elements of $\mathfrak{E}$,

$$f \equiv (f_1(x), f_2(x), \cdots), \qquad g \equiv (g_1(x), g_2(x), \cdots),$$

their E *sum*, written $f+g$, is defined to be identical with their D sum, that is,

$$f+g = (f_1(x)+g_1(x), f_2(x)+g_2(x), \cdots);$$

their E *product* fg is identical with their D product, and the *unity*, η, in E is the derived sequence

$$\eta \equiv (\eta_x(1),\ \eta_x(2), \cdots) \equiv (\eta_1(x),\ \eta_2(x), \cdots)$$

in $\mathfrak{R}$, where $\eta_x(n)$ is defined by

$$\begin{aligned} \eta_x(1) &= \text{the unity in } \mathfrak{R}_S, \\ \eta_x(n) &= \text{the zero in } \mathfrak{R}_S, \qquad n > 1. \end{aligned}$$

Hence it follows that E subtraction and division are the corresponding D operations.

Algebra $\mathfrak{E}$ is therefore the instance of algebra $\mathfrak{D}$ in which the elements are the set of all derived matrices of $\mathfrak{R}_S$ with the same argument x' together with the D sums and differences of these matrices.

The specific character of $\mathfrak{E}$, which distinguishes it from other instances of $\mathfrak{D}$, resides in $\mathfrak{E}$ composition, whereby any element of $\mathfrak{E}$ is decomposed (as in (5.2)) into an infinite number of primary factors; the fundamental theorem is contained in (5.8).

7. The algorithm of $\mathfrak{E}$. Since $\mathfrak{E}$ is an instance of $\mathfrak{D}$ we may replace operations upon elements (matrices) of $\mathfrak{E}$ by abstractly identical operations upon their D associated functions. Incidentally this at once suggests an n-fold generalization of $\mathfrak{E}$.

By a mere change in notation, replacing the letters s, x by r, t wherever they occur in § 3, we obtain from an initial matrix $r \equiv (r_1, r_2, \cdots)$ in $\mathfrak{S}$ its derived $t \equiv (t_1, t_2, \cdots, t_n, \cdots)$, corresponding to (3.6). Hence $t_1\, t_n = t_n$, $t_1 = t_\delta^0$, δ any prime. Precisely as in $\mathfrak{D}$ we treat the elements of t as parameters.

Take as the D associated function $f_\delta(t)$ of the primary f_δ in (4.1)

$$f_\delta(t) \equiv \sum_0^\infty t_\delta^n f_n(x_\delta). \tag{7.1}$$

Then, since $t_n \equiv t_\alpha^a\, t_\beta^b \cdots t_\gamma^c$ for n as in (3.4), we see from (5.1) that

$$\prod\nolimits_\delta [\sum\nolimits_0^\infty t_\delta^n f_n(x_\delta)] = \sum\nolimits_1^\infty t_n f_n(x), \tag{7.2}$$

the $\prod_\delta$ indicating the D product as δ runs through all primes >1. Either the product on the left of (7.2) or the sum on the right may be taken as the associated function in $\mathfrak{E}$ of (5.1), for if the left be distributed and rearranged with respect to the parameters $t_n (n = 1, 2, \cdots)$, as prescribed by $\mathfrak{D}$, we get the right identically.

The function associated with the C product K_δ in (5.4) is

$$\begin{aligned}(7.3)\quad &\{\textstyle\sum_0^\infty t_\delta^n f_n(x_\delta)\}\ \{\sum_0^\infty t_\delta^n g_n(x_\delta)\} \cdots \{\sum_0^\infty t_\delta^n h_n(x_\delta)\} \\ &\equiv \textstyle\sum_0^\infty t_\delta^n K_n(x_\delta),\end{aligned}$$

in which, by the definition of C multiplication,

$$(7.4)\qquad K_n(x_\delta) \equiv \sum f_a(x_\delta)\, g_b(x_\delta) \cdots h_c(x_\delta),$$

the $\sum$ referring to all sets of integers $a, b, \cdots, c$ each $\geqq 0$ whose sum is n.

With the D product K' in (5.6) is associated

$$\begin{aligned}(7.5)\quad &\{\textstyle\sum_1^\infty t_n f_n(x)\}\ \{\sum_1^\infty t_n g_n(x)\} \cdots \{\sum_1^\infty t_n h_n(x)\} \\ &\equiv \textstyle\sum_0^\infty t_n K_n'(x),\end{aligned}$$

where, by the definition of D multiplication,

$$(7.6)\qquad K_n'(x) \equiv \sum f_p(x)\, f_q(x) \cdots f_l(x),$$

the $\sum$ referring to all sets of integers $p, q, \cdots, l$ each $\geqq 1$ whose product is n.

It follows now from (7.2) that

$$(7.7)\qquad \textstyle\prod_\delta [\sum_0^\infty t_\delta^n K_n(x_\delta)] = \sum_1^\infty t_n K_n'(x),$$

the sign of equality having the significance explained in connection with D associated functions: after distribution of the left and rearrangement with respect to the parameters, the coefficient of t_n on the left is equal to that of t_n on

the right. Thus (7.7) is merely the formal equivalent, in terms of associated functions, of the matric equality (5.8).

8. Generators. We shall now replace multiplication and division in $\mathfrak{E}$ by abstractly identical operations upon functions of two variables t, ξ in $\mathfrak{A}$.

Let t, ξ be parameters in $\mathfrak{A}$, and recall that the zero, unity in $\mathfrak{A}$ are written 0, 1, also that sums, products, etc., are written without special notations, thus $t+\xi$, $t\xi$, etc. In the typical factor

$$\sum_0^\infty t_\delta^n f_n(x_\delta)$$

of the product in (7.2) replace t_δ by t, x_δ by ξ, and all operations in $\mathfrak{R}_S$ by the corresponding operations in $\mathfrak{A}$, so that

$$F(t, \xi) \equiv \sum_0^\infty t^n f_n(\xi) \tag{8.1}$$

is a function in $\mathfrak{A}$. By convention we assign to $f_0(\xi)$ the value 1 (= the unity in $\mathfrak{A}$), and call $F(t, \xi)$ the *generator* of the derived matrix

$$f \equiv (f_1(x),\ f_2(x), \cdots, f_n(x), \cdots) \tag{4.6}$$

in $\mathfrak{R}_S$. The following

$$F(t, \xi) \cdot \Gamma \cdot f, \quad \text{or} \quad F \cdot \Gamma \cdot f, \tag{8.2}$$

will be read "$F(t, \xi)$ generates f".

If $F \cdot \Gamma \cdot f$ and $G \cdot \Gamma \cdot g$ we define the generators F, G to be *equal*, $F = G$, only when $f = g$. It follows that $F = G$ implies the equality (in $\mathfrak{A}$), $(f_0(\xi), f_1(\xi), \cdots, f_n(\xi), \cdots) = (g_0(\xi), g_1(\xi), \cdots, g_n(\xi), \cdots)$.

Let $f, g, \cdots, h, \cdots$ be the set of all derived matrices in $\mathfrak{R}_S$ having the same argument; their respective generators are $F(t, \xi)$, $G(t, \xi)$, $\cdots$, $H(t, \xi)$, $\cdots$. Then, with respect to C multiplication the set of all generators $F, G, \cdots, H$ is an abelian group $\mathfrak{G}$.

Denoting multiplication in $\mathfrak{G}$ by juxtaposition, thus $FG \cdots H$, we see that $FG \cdots H$ *generates the E product*

$fg \cdots h$, and if F^{-1} be the inverse of F in $\mathfrak{G}$, then $F^{-1} \cdot \Gamma \cdot f^{-1}$, where $f^{-1} \equiv \eta/f$ is the E reciprocal of f.

Hence the properties of elements of $\mathfrak{E}$ with respect to multiplication are implied by the like for $\mathfrak{G}$, and may be written down therefrom by replacing the symbol of each generator by the derived matrix in $\mathfrak{R}_S$ which it generates.

In applying the last theorem it is necessary to have a short way of getting the derived matrix f generated by a given $F(t, \xi)$ and also of constructing the generator $F(t, \xi)$ of a given f. For the first it is sufficient to determine $f_n(x)$ when $F(t, \xi)$ is known. Write

$$f_n(x) = f_a(x_\alpha)\, f_b(x_\beta) \cdots f_c(x_\gamma), \tag{8.3}$$

where (as before) $n = \alpha^a \beta^b \cdots \gamma^c$ is the resolution of n into prime factors. Since $F(t, \xi)$ is given, so also is the explicit form of $f_n(\xi)$. In $f_n(\xi)$ put $(n, \xi) = (a, x_\alpha), \cdots, (c, x_\gamma)$ and get $f_a(x_\alpha), \cdots, f_c(x_\gamma)$, and hence $f_n(x)$. Conversely, to find $F(t, \xi)$ from (8.3), replace (a, x_α) in $f_a(x_\alpha)$ by (n, ξ), multiply the resulting $f_n(\xi)$ by t^n and sum for $n = 0$ to ∞; then $F(t, \xi) = \sum_0^\infty t^n f_n(\xi)$. Note that *the first term of any generator is the unity*, 1, *in* $\mathfrak{A}$.

9. Arithmetic in $\mathfrak{E}$. The derived matrix f is said to be *algebraic* or *transcendental* in $\mathfrak{E}$ according as its generator $F(t, \xi)$ is an algebraic or a transcendental function of t, ξ in $\mathfrak{A}$, and the corresponding generators are similarly named. To include numerous special theories we now frame a definition of fundamental domains.

Let the $f_j(\xi)$ $(j = 1, \cdots, n)$ be algebraic functions in $\mathfrak{A}$, where n is a finite integer > 0. Then

$$F(t, \xi) = 1 + t f_r(\xi) + \cdots + t^n f_n(\xi)$$

is a polynomial in t and $F(t, \xi)$ is an algebraic generator. Let $c \neq 0$ be in $\mathfrak{A}$. Then the algebraic function $F(t, \xi) + c$ in $\mathfrak{A}$ is not a generator, since the term independent of t is $\neq 1$ (the unity in $\mathfrak{A}$). An algebraic generator, such as the

above $F(t, \xi)$, which is a polynomial in t is called *fundamental*. The essential point in this definition is the finiteness of the degree in t. *The set of all fundamental generators is closed under multiplication in* $\mathfrak{A}$.

Let $F(t, \xi)$ be any fundamental generator. Then if $F(t, \xi)$ is the product in $\mathfrak{A}$ of fundamental generators with coefficients in the domain ∇, the generator is said to be *reducible* in ∇, otherwise *irreducible*.

Suppose now that each fundamental generator is the product in $\mathfrak{A}$ of fundamental generators irreducible in ∇ in one way only, apart from permutations of the factors. Then ∇ is called a *fundamental domain*. In what follows it is assumed that such a ∇ exists. An instance is ∇ the domain of rational integers for the special and important case in which the generators are polynomials in both ξ and t.

If $F \cdot \Gamma \cdot f$, then $1/F \cdot \Gamma \cdot f'$, where $\cdot f' = \eta/f$, the reciprocal in $\mathfrak{E}$ of f, η being the unity in $\mathfrak{E}$; if F is fundamental, f is called *fundamental*, and η/f the *reciprocal* of f; both f and η/f are called *prime or composite in* $\mathfrak{E}$ according as F is irreducible or reducible. Since $\eta g = g$, where g is any element of $\mathfrak{E}$, unit factors η are disregarded, and the like is to hold in what follows.

A generator G obtained from a finite number of fundamental generators by a finite number of multiplications and divisions (in $\mathfrak{A}$) will be called *rational*; if $G \cdot \Gamma \cdot g$, then g is called *rational in* $\mathfrak{E}$.

The set of all rational derived matrices in $\mathfrak{E}$ *is an abelian group, say* $\mathfrak{G}_E$, *under* E *multiplication.*

If $F \cdot \Gamma \cdot f$ we define f^r by $F^r \cdot \Gamma \cdot f^r$, and clearly $F^{-r} \cdot \Gamma \cdot f'^r$, where $f' = \eta/f$. Let $F = G^a H^b \cdots K^c$ be the resolution (in ∇) of the fundamental generator F into a product of powers of distinct irreducible fundamental generators $G, H, \cdots, K$. Note that f^r as just defined is the D product of r derived matrices (in $\mathfrak{E}$) each equal to f. The D product of several such powers $g^a, h^b, \cdots, k^c$ of derived matrices will be indicated by juxtaposition, $g^a h^b \cdots k^c$, so that the last is an element of $\mathfrak{E}$ and (see § 6) is indeed the E product of the ath,

bth, $\cdots$, cth powers $g, h, \cdots, k$ in $\mathfrak{E}$. For $F, \cdots, K$ as above, it follows that if

$$F \cdot \Gamma \cdot f, \; G \cdot \Gamma \cdot g, \; H \cdot \Gamma \cdot h, \cdots, \; K \cdot \Gamma \cdot k,$$

then

$$f = g^a h^b \cdots k^c, \qquad \eta / f = \eta / g h \cdots k,$$

and further that these resolutions are unique. We shall abbreviate the E product of f and η / g to f / g.

A generator F obtained from a finite number of fundamental generators by a finite number of multiplications will be called *integral*; if $F \cdot \Gamma \cdot f$ then f is called an *integral element in* $\mathfrak{E}$, and f is prime or composite in Γ. Hence we see that *any integral f in $\mathfrak{E}$ is the product of prime integral elements in $\mathfrak{E}$ in one way only* (apart from permutations of the factors), also that *the reciprocal of the integral element f in $\mathfrak{E}$* is uniquely the product of reciprocals of prime integral elements in $\mathfrak{E}$. Hence *any element of $\mathfrak{E}$ whose generator is in $\mathfrak{G}_E$ has* (apart from powers of the unit η) *a unique resolution of the form*

$$g^a h^b \cdots k^c / l^d m^e \cdots n^t,$$

where $g, h, \cdots, k, l, m, \cdots, n$ are prime elements in $\mathfrak{E}$, and the exponents are integers > 0.

For convenience we define $f^0 = \eta$, where f is any element of $\mathfrak{E}$. The above shows merely one kind of arithmetic that can be obtained from $\mathfrak{E}$. Primes and irreducibility can obviously be defined in many other ways to yield in $\mathfrak{E}$ the fundamental theorem of arithmetic. The above was selected because of its immediate applicability to the coördination and extension of the algebraic properties of a large body of existing arithmetical functions, as will be briefly indicated in the following sections.

THE VARIETY $\mathfrak{E}_r$ OF $\mathfrak{E}$, § 10–12

10. Simplifications of $\mathfrak{E}$ for rational integers. To apply $\mathfrak{E}$ to functions of rational integers take $x_p = p$ (p any prime) in (3.2), and hence $x_n = n$ in (3.5) and everywhere

in $\mathfrak{E}$. This determines a variety, which we shall denote by $\mathfrak{E}_r$, of $\mathfrak{E}$. There is still a wide choice in the definition of $f_x(n)$ $\quad f_n(x)$ of (4.4) in $\mathfrak{E}_r$. The following will suffice for purposes of illustration. Since now $x_p = p$ for p prime we take

$$f_n(x_p) \equiv f_n(p) \qquad (p \text{ prime} > 1,\ n = 0,\ 1,\ \cdots)$$

and (see § 4), $f_0(p) = 1$. For this choice (4.4) now defines the function $f_x(n) \equiv f(n)$ in $\mathfrak{E}_r$,

$$f(n) \equiv f_a(\alpha) f_b(\beta) \cdots f_c(\gamma), \qquad f(1) = 1,$$

where $n = \alpha^a \beta^b \cdots \gamma^c$ is as before the resolution of $n > 1$ into primes. In §§ 7, 8 we now have $x_\delta = \delta$ (δ any prime > 1), and (7.2) becomes

$$\prod\nolimits_\delta [1 + \sum\nolimits_1^\infty t_\delta^n f_n(\delta)] = \sum\nolimits_1^\infty t_n f(n),$$

in which, to obtain the corresponding generator, we replace δ by ξ and t_δ by t. The generating identity becomes

$$F(t, \xi) \cdot \Gamma \cdot f, \qquad F(t, \xi) \equiv 1 + \sum\nolimits_1^\infty t_n f_n(\xi),$$

and the specific forms of the $f_n(\xi)$ are still at our disposal. Before specializing we introduce some simplifications appropriate to $\mathfrak{E}_r$.

As a working device we note first that by the definition of matric equality,

$$(f(1), f(2), \cdots, f(n), \cdots) = (g(1), g(2), \cdots, g(n), \cdots),$$

which states the equality of derived matrices in $\mathfrak{E}_r$ corresponding to those defined in $\mathfrak{E}$ by (4.6), is equivalent to

$$f(n) = g(n) \qquad (n = 1, 2, \cdots).$$

In the last we may drop the reference to the range $1, 2, \cdots$ of n, write simply $f(n) = g(n)$, and understand by this the

implied matric equality in $\mathfrak{E}_r$. Hence the equality $f = gh \cdots k$ in $\mathfrak{E}_r$ is equivalent to

$$f(n) = P_D(g(n), h(n), \cdots, k(n)),$$

and this in full (on supplying the definition of the D product indicated) is

$$f(n) = \sum g(d_1)\, h(d_2) \cdots k(d_s),$$

the $\sum$ referring to all sets $(d_1, d_2, \cdots, d_s)$ of integers $d_1, d_2, \cdots, d_s$ each >0 whose product is n, where $s =$ the number of functions $g, h, \cdots, k$.

The unity in $\mathfrak{E}_r$ is η, where $\eta(n) = 1$ or 0 according as $n = 1$ or $n > 1$. If f is any element of $\mathfrak{E}_r$, $\eta f = f$, the product and the equality having the meanings just explained; the reciprocal f' of f is uniquely defined by $ff' = \eta$.

To write down the generator of $f(n)$ we have in any given instance the specific forms of the functions

$$f_a(p), \quad (p \text{ prime} > 1,\ a = 0, 1, \cdots),$$

with $f_0(p) = 1$, and hence from the resolution $n = \alpha^a \beta^b \cdots \gamma^c$ we get by the definition of $f(n)$,

$$f(n) = f_a(\alpha)\, f_b(\beta) \cdots f_c(\gamma);$$

whence, from the properties of the parameters t_δ, t_n in $\mathfrak{D}$ we have

$$\prod\nolimits_\delta [1 + \sum\nolimits_1^\infty t_\delta^n f_n(\delta)] = \sum\nolimits_1^\infty t_n f(n)$$

on observing that $t_n = t_\alpha^a t_\beta^b \cdots t_\gamma^c$ and noting the coefficient of t_n in the distributed form of the left, so that, replacing (t_δ, δ) by (t, ξ), we get the required generator

$$F(t, \xi) = 1 + \sum\nolimits_1^\infty t^n f_n(\xi).$$

Conversely, from this generator, reversing the steps just outlined, we find the $f(n)$ generated by $F(t, \xi)$. We have

insisted on these extremely simple details because the applications of $\mathfrak{E}_r$ involve nothing more complicated.

The specialization of the above in which the $f_n(\xi)$ $(n = 1, 2, \cdots)$ are polynomials in ξ, or in which all but a finite number of them vanish identically and the rest are polynomials, cover practically all of the important arithmetical functions in the literature of unique factorization in rational arithmetic. The following short selection will illustrate operations in $\mathfrak{E}_r$ and prepare the way for the statement of a generalization of $\mathfrak{E}$.

11. **Certain functions in $\mathfrak{E}_r$.** The most immediate applications of $\mathfrak{E}_r$ are to the extensive literature summarized in Dickson's *History*, vol. I, chapters V, X, XIX, and to functions of $[x]$, the greatest integer $\leqq x$ (this section of arithmetic has not been reported in the published parts of the *History*). These applications concern relations between functions of divisors, the inversion of such relations and of series, generalizations of Euler's φ function and others, numerical integrals and derivatives (these are merely a very special case of multiplication and division in $\mathfrak{E}_r$ and have no characteristic properties which distinguish them from other similar operations in $\mathfrak{E}_r$), and many similar topics, the majority of which $\mathfrak{E}_r$ reduces to a simple, coherent system abstractly identical with the simplest parts of $\mathfrak{A}$. We need give only enough to illustrate the use of generators. The notation is as in § 10. Unless otherwise stated prime shall mean prime > 1, and the functions considered exist only for integral values > 0 of their arguments. By nth power is meant the nth power of an integer > 0.

If m, n are coprime integers > 0 and $f(mn) = f(m)\,f(n)$, f is called *factorable*. The examples in this paragraph are confined to factorable functions. If n is divisible by no square > 1 it is called *simple*. Any integer $n > 1$ has a unique resolution into a product of coprime simple numbers whose exponents are distinct, $n = P^a Q^b \cdots R^c$, where $P, Q, \cdots, R$ are simple and coprime, and $a > b > \cdots > c$. If $n = p_1^{a_1} \cdots p_s^{a_s}$ is the resolution of n into powers of distinct primes, we call

(after Sylvester) $\lambda(n) \equiv a_1 + a_2 + \cdots + a_s$ the *multiplicity* of n, and $\gamma(n) = s$ the *manifoldness* of n. Hence $\lambda(n)$, $\gamma(n)$ are respectively the total number, and the number of distinct primes that divide n. A great many of the arithmetical functions in the literature are special cases of the following, or are products in $\mathfrak{E}_r$ of positive or negative integral powers of it:

(11.1) $$\Psi(n;\, a,\, b,\, c) = 0$$

if n is not the bth power of a simple number; in the contrary case the value of the function is $c^{\gamma(n)}\, n^{a,b}$. From this definition we write down its generator,

(11.2) $$(1 + c\,\xi^a\, t^b) \cdot \Gamma \cdot \Psi(n;\, a,\, b,\, c)$$

and hence that of its reciprocal Ψ',

(11.3) $$(1 + c\,\xi^a\, t^b)^{-1} \cdot \Gamma \cdot \Psi'(n;\, a,\, b,\, c).$$

The verbal definition of Ψ' is read off from the expansion

$$1 - c\,\xi^a\, t^b + c^2\,\xi^{2a}\, t^{2b} - c^3\,\xi^{3a}\, t^{3b} + \cdots$$

of the generator, and is

(11.4) $$\Psi'(n;\, a,\, b,\, c) = 0$$

if n is not the bth power of an integer (not necessarily simple); in the contrary case the function has the value $(-c)^{\lambda(m)}\, n^{a/b}$, where $m = n^{1/b}$. If s is an integer $\gtrless 0$ we indicate the sth power in $\mathfrak{E}_r$ of Ψ as in (11.1) by writing $\Psi^s(n;\, a,\, b,\, c)$ and so in all like cases. Hence

$$\Psi'^s(n;\, a,\, b,\, c) = \Psi^{-s}(n;\, a,\, b,\, c).$$

From the definition of reciprocals in $\mathfrak{E}_r$ we have

(11.5) $$P_D(\Psi^s(n;\, a,\, b,\, c),\ \Psi^{-s}(n;\, a,\, b,\, c)) = \eta(n),$$

since the generators of Ψ^s, Ψ^{-s} are the reciprocals $(1 + c\,\xi^a\, t^b)^s$, $(1 + c\,\xi^a\, t^b)^{-s}$ in $\mathfrak{A}$. In full (11.5) states that

$$\sum \Psi^s(d; a, b, c)\ \Psi^{-s}(\delta; a, b, c) = \eta(n),$$

the summation extending to all pairs (d, δ) of divisors each >0 of n such that $d\delta = n$. The abbreviated form of (11.5) is $\Psi^s \Psi^{-s} = \eta$.

To see that Ψ and its powers in $\mathfrak{E}_r$ contain many of the known arithmetical functions we first specialize as follows, defining six subcases.

(11.6) $\psi(n; a, b,) \equiv \Psi(n; a, b, -1)$, $= 0$ if n is not the bth power of a simple number and otherwise $= \pm n^{a/b}$ according as the manifoldness of n is even or odd.

(11.7) $\psi^{-1}(n; a, b) = 0$ or $n^{a/b}$ according as n is or is not a bth power.

(11.8) $\chi(n; a, b) \equiv \Psi(n; a, b)$, $= 0$ or $n^{a/b}$ according as n is not or is the bth power of a simple number.

(11.9) $\chi^{-1}(n; a, b) = 0$ if n is not a bth power, and otherwise $= \pm n^{a/b}$ according as the multiplicity of $n^{1/b}$ is even or odd.

(11.10) $\zeta(n; a, b) \equiv \Psi(n; 0, b, a)$, $= 0$ or $a^{\gamma(n)}$ according as n is not or is the bth power of a simple number.

(11.11) $\zeta^{-1}(n; a, b) = 0$ if n is not a bth power, and in the contrary case $= \pm a^{\lambda(m)}$, $m \equiv n^{1/b}$, according as the multiplicity of m is even or odd.

The generators are written down from these definitions or at once from (11.2), (11.3):

$$\begin{array}{ll} (1-\xi^a t^b)\cdot \Gamma\cdot \psi, & (1-\xi^a t^b)^{-1}\cdot \Gamma\cdot \psi^{-1}, \\ (1+\xi^a t^b)\cdot \Gamma\cdot \chi, & (1+\xi^a t^b)^{-1}\cdot \Gamma\cdot \chi^{-1}, \\ (1+a t^b)\cdot \Gamma\cdot \zeta, & (1+a t^b)^{-1}\cdot \Gamma\cdot \zeta^{-1}, \end{array} \tag{11.12}$$

the second column being of course superfluous—it is included merely for ease in verifying the special cases given presently.

To illustrate in passing one way in which generators are used, we have as the equivalent, in $\mathfrak{E}_r$ of the identity

$$1-\xi^{2a} t^{2a} = (1-\xi^a t^b)(1+\xi^a t^b)$$

in $\mathfrak{A}$ the following,

$$P_D(\psi(n; a, b), \chi(n; a, b)) = \psi(n; 2a, 2b).$$

Particularizing these again, and introducing the customary notations for such of the functions as are current, we write

$\mu(n) = 0$ if n is not simple, otherwise 1 or -1 according as the manifoldness of n is even or odd (Möbius' function);

$\mu_{1/a}(n) \equiv \mu(n^{1/a})$, which exists only when n is an ath power;

$k_r(n) = 1$ or 0 according as n is or is not an rth power;

$u_r(n) \equiv n^r$, defined for all real values of n, r, and $u_1(n^{1/2}) \equiv u_{1/2}(n)$ and similarly for higher roots than the second;

$\pi(n) = 1$ or -1 according as the multiplicity of n is even or odd, $\pi(n) = (-1)^{\lambda(n)}$;

$\nu(n) =$ the number of divisors of n;

$\varphi(n) =$ the totient of n, $=$ the number of integers $\leqq n$ and coprime with n;

$\sigma(n) =$ the sum of the divisors of n;

$\theta(n) =$ the total number of decompositions of n into a pair of coprime factors, the order of the factors being considered. These are but a few of the special cases of Ψ and its powers, From them we get

$$
\begin{aligned}
\psi(n;\ a, b) &= k_b(n)\ \mu_{1/b}(n)\ u_{a/b}(n), \\
\psi^{-1}(n;\ a, b) &= k_b(n)\ u_{a/b}(n), \\
\chi(n;\ a, b) &= k_b(n)\ \{\mu_{1/b}(n)\}^2\ u_{a/b}(n), \\
\chi^{-1}(n;\ a, b) &= (-1)^{\lambda(m)}\ k_b(n)\ u_{a/b}(n) \quad (m \equiv n^{1/b}), \\
\zeta(n;\ a, b) &= \{\mu_{1/b}(n)\}^2\ k_b(n)\ a^{\nu(n)}, \\
\zeta^{-1}(n;\ a, b) &= (-a)^{\lambda(m)}\ k_b(n) \qquad (m \equiv n^{1/b}).
\end{aligned}
\tag{11.13}
$$

Before writing down the generators of special cases of these we must recall the absolute product $|fg|$ of $f \equiv (f(1), f(2), \cdots)$, $g \equiv (g(1), g(2), \cdots)$. Put $|fg| = h$ for the moment. Then (see chapter I § 8), $h(n) = g(n)\,g(n)$ $(n = 1, 2, \cdots)$. Hence $|f^2| = |ff|$, $f^3, \cdots$ are defined. These will not be confused with the products and powers fg, $g^2, \cdots$ in $\mathfrak{E}_r$, which (as explained above) are products P_D. For example ν^2, $|\nu^2|$ are distinct functions,

$$\nu^2(n) = \sum \nu(d)\ \nu(\delta), \qquad |\nu^2|(n) = \{\nu(n)\}^2,$$

the summation referring as before to all pairs of conjugate divisors d, δ of n.

It will suffice to write down the generators of only a few. We see from the above, or directly from the definitions, the following:

FUNCTION,	GENERATOR	FUNCTION,	GENERATOR
μ,	$1-t$,	$\lvert u_1 \nu \rvert$,	$(1-\xi t)^{-2}$,
$\lvert \mu^2 \rvert$,	$1+t$,	$\lvert \nu^2 \rvert$,	$(1+t)(1-t)^{-3}$.
ν,	$(1-t)^{-2}$,	$\lvert \mu^2 \nu \rvert$,	$1+2t$,
φ,	$(1-t)(1-\xi t)^{-1}$.	$\pi\theta$,	$(1-t)(1+t)^{-1}$.
θ,	$(1+t)(1-t)^{-1}$,	$\lvert \pi u_r \rvert$,	$(1+\xi^r t)^{-1}$.
π,	$(1+t)^{-1}$,	$\lvert \pi \nu \rvert$,	$(1+t)^{-2}$,
k_r,	$(1-t^r)^{-1}$,	$\lvert u_r \nu \rvert$,	$(1-\xi^r t)^{-2}$,
σ,	$(1-t)^{-1}(1-\xi t)^{-1}$,	$\lvert \pi\sigma \rvert$,	$(1+t)^{-1}(1+\xi t)^{-1}$,
u_r,	$(1-\xi^r t)^{-1}$,	$\lvert \theta^r \rvert$,	$\{1+(2^r-1)t\}(1-t)^{-1}$.
$\lvert \mu u_r \rvert$,	$1-\xi^r t$,	$\lvert u_1 \sigma \rvert$,	$(1-\xi t)^{-1}(1-\xi^2 t)^{-1}$,
$\lvert \mu^2 u_r \rvert$,	$1+\xi^r t$,		

and the list may be continued indefinitely. This illustrates the richness of ψ, which is itself one of the simplest algebraic generators in $\mathfrak{E}_r$.

If we take ∇ of § 9 to be the rational domain, it follows from the foregoing generators that μ, $\lvert \mu^2 \rvert$, π, $\lvert \mu^2 \nu \rvert$, u_r, $\lvert \pi u_r \rvert$, are primes in $\mathfrak{E}_r$, and that we have the following resolutions into primes in $\mathfrak{E}_r$;

$$\nu = u_0^2, \quad \varphi = \mu u_1, \quad \sigma = u_0 u_1, \quad \theta = \lvert \mu^2 \rvert u_0,$$
$$\lvert \pi\theta \rvert = \mu\pi, \quad \lvert u_1 \nu \rvert = u_1^2, \quad \nu^2 = \lvert \mu^2 \rvert u_0^3, \quad \lvert \pi\sigma \rvert = \pi \lvert u_1 \pi \rvert,$$
$$\lvert u_1 \sigma \rvert = u_1 u_2, \quad \lvert u_r \nu \rvert = u_r^2,$$

and many more by inspection. For example the resolution of θ into the product of the primes $\lvert \mu^2 \rvert$, u_0 is equivalent to the identity in $\mathfrak{A}$ between generators

$$(1+t)(1-t)^{-1} = (1+t) \times (1- \quad)^{-1},$$

and read in full the resolution $\theta = \lvert \mu^2 \rvert u_0$ in $\mathfrak{E}_r$ states the relation $\theta(n) = \sum \{\mu(d)\}^2$,

the $\sum$ referring to all divisors d of n, since $u_0(\delta) = 1$ for all integers $\delta > 0$.

Having resolved a given set of elements of $\mathfrak{E}_r$ into their prime factors we may then proceed, precisely as in $\mathfrak{A}$, to obtain from them by operations in $\mathfrak{E}_r$, of which multiplication and division lead to the more interesting results, chains of relations between functions of divisors. We shall illustrate this in a moment. For the present we remark that the equivalent in $\mathfrak{E}_r$ of the associative law of multiplication in $\mathfrak{A}$ leads to interesting consequences. Thus, if $f_j (j = 1, 2, \cdots, s)$ are elements of $\mathfrak{E}_r$, their product f is in $\mathfrak{E}_r$, and likewise for $f_a f_b \cdots f_c$, where $a, b, \cdots, c$ are any integers chosen from $1, 2, \cdots, s$. Each such product defines a function whose verbal definition can be read off from its generator, and the function so defined will in general isolate properties of divisors sufficiently different from those defined by its factors to make it of interest. For example, the product μu_1 may be replaced wherever it occurs by q. Regarding f as a product in all possible ways given by the associative law, thus $f_1 \cdot f_2 \cdots f_s$, $f_1 f_2 \cdot f_3 f_4 \cdots f_s$, etc., we obtain its structure in $\mathfrak{E}_r$ with reference to $\Pi(s)$ distinct arithmetical functions, where $\Pi(s)$ is the enumerative function of chapter 1, § 26. Again, the most obvious consequences of division in $\mathfrak{A}$ imply relations in $\mathfrak{E}_r$ which are not always obvious at first sight. Division in $\mathfrak{A}$, that is, division of generators in the present instance, may be replaced at once by division in $\mathfrak{E}_r$, since the processes are abstractly identical, and likewise for multiplication. For example, suppose f, g, h, k, p, q are elements of $\mathfrak{E}_r$ between which there are the relations

$$fg = hk, \qquad fp = hq.$$

Then, by elimination of f, h, precisely as in $\mathfrak{A}$, we infer $gq = pk$. This almost trivial example in $\mathfrak{E}_r$ illustrates the simplicity and power of the method. For, stating the theorem in common notation we have the following: the relations

$$\sum f(d)\, g(\delta) = \sum h(d)\, k(\delta) \qquad \sum f(d)\, p(\delta) = \sum h(d)\, q(\delta)$$

together imply

$$\sum g(d)\, g(\delta) = \sum p(d)\, k(\delta),$$

where $f, \cdots, g$ are arbitrary single valued functions of integers, and $\sum$ refers (as before) to all pairs of conjugate divisors d, δ of n. As another, similar, example we see that $u_0 f = g$ implies $f = g/u_0 = g\mu$, since (by their respective generators $1-t$, $(1-t)^{-1}$ given above) μ, u are reciprocals, so that $\mu u_0 = \eta$. But this is the important inversion theorem of Dedekind, namely

$$\sum f(d) = g(n) . \supset . f(n) = \sum g(d)\mu(\delta).$$

This theorem (which as a very special instance of division in $\mathfrak{E}_r$) has therefore the immediate extension to any functions f, g, h,

$$fg = h . \supset . g = h/f \text{ and } f = h/g,$$

or, if f^{-1}, g^{-1} denote as usual the reciprocals of f, g in $\mathfrak{E}_r$, from $fg = h$ we infer $f = hg^{-1}$, $g = hf^{-1}$, exactly as in $\mathfrak{A}$.

Returning to the special functions we have the following illustrations of the above remarks,

$$\begin{aligned}
u_0\varphi &= u_0\mu u_1 &&= u_1.\\
u_0\sigma &= u_0^2 u_1 &&= \nu u_1,\\
u_0 | u_1\sigma | &= u_0 u_1 u_2 &&= u_2\sigma,\\
\nu\theta &= |\mu^2| u_0^3 &&= |\nu^2|,\\
\nu^2 &= u_0^4 &&= u_0^4\pi|\mu^2| = u_0\pi|\mu^2| u_0^3 = k_2|\nu^2|,\\
\varphi\nu &= \mu u_1 u_0^2 &&= u_1 u_0 = \sigma.\\
\sigma^2 &= u_0^2 u_1^2 &&= \nu u_1\nu,\\
|\pi\theta|\nu &= \mu\pi u_0^3 &&= u_0\pi = k_2,\\
\pi\nu &= \pi u_0^2 &&= u_0 k_2,
\end{aligned}$$

and so on indefinitely. Again, each of the following, and hence all products and quotients of positive integral powers of any number of them, is equal to η, the unit in $\mathfrak{E}_r$,

$$\mu u_0, \quad \mu k_1, \quad u_r | \mu u_r |, \quad \pi | \mu^2 |, \quad \mu^2 \nu, \quad | \mu u_1 | \varphi u_0,$$
$$| \mu u_1 | \mu \sigma, \quad \pi \mu \theta, \quad | \pi u_1 | u_1 \mu^2, \quad \mu u_r \; u_r,$$

and so on. To see one of these in full, consider $\pi \mu \theta$. Then $\pi \mu \theta = \eta$ states that

$$\sum \pi(d_1) \, \mu(d_2) \, \theta(d_3) = 1 \text{ or } 0$$

according as $n = 1$ or $n > 1$, the $\sum$ referring to all triples (d_1, d_2, d_3) of divisors of n such that $d_1 d_2 d_3 = n$. All these are instances of (11. 5).

These few examples are sufficient to show one direction in which $\mathfrak{E}_r$ may be used to coördinate and indefinitely extend one part of the algebra of arithmetical functions. We pass on to illustrations of different types.

12. **Miscellaneous applications of $\mathfrak{E}_r$.** Again we make only a short selection, as the abstract identity of $\mathfrak{E}_r$ and $\mathfrak{A}$ suggests inexhaustible possibilities which, however interesting in themselves, add nothing to the comprehensive theorem that $\mathfrak{E}_r$, $\mathfrak{A}$ are abstractly identical. We shall endeavor to choose examples that have some importance in other departments of arithmetic.

Consider first the arithmetical inversion of products, an instance of which occurs in the determination of the equation of primitive roots. We have defined f^a, where f is in $\mathfrak{E}_r$ and a is an integer ($\gtreqless 0$). By obvious means, precisely as in $\mathfrak{A}$, we can extend the definition to powers whose exponents are any rational numbers. But it is more interesting to generalize in another direction, and we shall define f^g, where f, g are any elements of $\mathfrak{E}_r$ to be the product

$$f^g = \prod [f(d)]^{g(\delta)} \tag{12.1}$$

where $\prod$ refers to all pairs (d, δ) of conjugate divisors of n. As before we omit from $f^g = f^g(n)$ the symbol of the argument n, and an equality

$$f^g = h^k, \tag{12.2}$$

where f, g, h, k are in $\mathfrak{E}_r$, is to be understood in the matric sense

$$f^g(n) = h^k(n) \qquad (n = 1, 2, \ldots).$$

Let g', k' be the respective reciprocals of g, k, so that $gg' = kk' = \eta$ (the unit in $\mathfrak{E}_r$). Then we have the *general inversion of functional powers in* $\mathfrak{E}_r$, expressed in the following (12.2) *implies*

(12.3) $$f^{k'} = h^{g'}.$$

Observe first that if for the moment f, g, h, k be interpreted as elements of $\mathfrak{A}$, so that $g' = 1/g$, $k' = 1/k$, the theorem is true. Hence the inversion in $\mathfrak{E}_r$ is abstractly identical with the extraction of roots in $\mathfrak{A}$—the arithmetical roots being understood in $\mathfrak{A}$. The inversion in $\mathfrak{E}_r$ is proved immediately by taking logarithms in (12.2) and multiplying in $\mathfrak{E}_r$ the result by the arbitrary element φ of $\mathfrak{E}_r$,

$$\varphi g F = \varphi k H \,(\log f(n) \equiv F(n),\ \log h(n) = H(n));$$

whence $f^{\varphi g} = h^{\varphi k}$, and therefore, on chosing $\varphi = g'k'$ we get (12.3).

If in the above we take $g \equiv u_0$, $k \equiv \eta$, we see that

(12.4) $$f^{u_0} = h^{\eta} \ .\supset. \ f^{\eta} = h^{\mu},$$

or, in non-symbolic form,

(12.41) $$\prod f(d) = h(n) \ .\supset. \ f(n) = \prod [h(d)]^{\mu(\delta)}$$

a theorem of Dedekind, first used in the theory of binomial congruences by Gauss and Cauchy.

Consider next the inversion of series, and for brevity assume that all the series discussed are infinite and convergent. Write

(12.5) $$F(j) \equiv \sum_{i=1} h(i) f(ij).$$

Let h' be the reciprocal in $\mathfrak{E}_r$ of h; multiply (12.5) throughout by $h'(j)$ and take the sum with respect to $j = 1, 2, \cdots$. Then we see that (12.5) implies

$$f(1) = \sum_{j=1} h'(j)\, F(j). \tag{12.6}$$

The pair (12.5), (12.6) may be considered as inversions of each other.

A special case of the last is of interest. We note particularly that it is a specialization and not, in spite of its appearance, a generalization of the preceding. With Cesàro (see Dickson's *History*, loc cit. for references) let $\varepsilon_1(x) = x$, and let $\varepsilon_\alpha(x)$, $\varepsilon_\beta(x)$, $\cdots$ ($\alpha, \beta, \cdots = 1, 2, \cdots$) denote single valued functions of x such that, if α, β are any intergers > 0,

$$\varepsilon_\alpha(\varepsilon_\beta(x)) = \varepsilon_{\alpha\beta}(x) = \varepsilon_\beta(\varepsilon_\alpha(x)),$$

and let $f, g, h, \cdots$ be any elements of $\mathfrak{E}_r$ ($\equiv$ functions taking single definite values for integral values ≥ 0 of their arguments). Then we may write, as in developing $\mathfrak{E}$,

$$f(\varepsilon_n(x)) \equiv f_n(x) \equiv f_x(n)$$

and consider the first of these as the particular element $f_x(n)$ of $\mathfrak{E}_r$. Thus, defining $g_x(n)$, $h_x(n)$, $\cdots$ similarly, we see that $f_x, g_x, h_x, \cdots$ are instances of the arbitrary $f, g, h, \cdots$ in $\mathfrak{E}_r$. *Hence if between such $f, g, h, \cdots$ we have established a relation R in $\mathfrak{E}_r$, an instance R' of R is obtained on supplying to each function the suffix x with the above meaning, and conversely from R' may be inferred R if we take $\varepsilon_n(x) \equiv nx$ and in the result set $x = 1$, as clearly is permissible by the definition of the ε's. Hence R, R' are formally equivalent, and R can be written down from R' by dropping the suffix x.*

Now let $\Omega^A(x) = 1$ or 0 according as the integer $x > 0$ is or is not a member of the class A, and consider only classes A such that

$$\Omega^A(x)\,\Omega^A(y) = \Omega^A(xy),$$

and hence $\Omega^A(1) = 1$. Then, the meaning of the absolute product $|fg|$, for any elements f, g of $\mathfrak{E}_r$, being as before (see § 11), we have

$$\Omega^A(\varepsilon_n(x)) \quad \Omega_x(n), \qquad f(\varepsilon_n(x)) \qquad f_x(n),$$

and therefore $|\Omega_x^A f_x|$ is defined. It follows that *in any relation R between arbitrary elements $f, g, h, \cdots$ of $\mathfrak{E}_r$, we may obtain a formally equivalent relation R' on replacing these by*

$$|\Omega_x^A f_x|, \qquad |\Omega_y^B g_y|, \qquad \Omega_z^C h_z . \qquad \cdots$$

respectively, where $A, B, C, \cdots$ are any classes of integers, $x, y, z, \cdots$ any variables, and $\varepsilon_\alpha(x)$, $\varepsilon_\beta(y)$, $\varepsilon_\gamma(z)$, $\cdots$ ($\alpha, \beta, \gamma, \cdots = 1, 2, \cdots$) any sets of functions having the group property as defined for $\varepsilon_\alpha(x)$. It is to be noted that the variables are not necessarily independent, nor the $\varepsilon_\alpha(x)$, $\varepsilon_\beta(y)$, $\cdots$ necessarily distinct, and that $A, B, C, \cdots$ are not necessarily mutually exclusive. *To pass from R' back to R take $\varepsilon_\alpha(x) = \alpha x$, $\varepsilon_\beta(y) = \beta y$, $\cdots$ ($\alpha, \beta = 1, 2, \cdots$), $A = B = C = \cdots$ = the class of all integers > 0, and in the result put $x = y = z = \cdots = 1$.*

Noting that the reciprocal in $\mathfrak{E}_r$ of $\Omega^A(n)h(n)$ is $\Omega^A(n)h'(n)$, where h' is the reciprocal of h, we see that the inversion of (12.5) into (12.6) implies and is implied by the following.

$$F_x(1) = \sum_{i=1} \Omega^A(i)h(i)f_x(i) \tag{12.7}$$

implies

$$f_x(1) = \sum_{i=1} \Omega^A(i)h'(i)F_x(i). \tag{12.8}$$

If in this we replace the functions with suffix x by their full definitions,

$$F_x(1) = F(x), \qquad f_x(i) = f((\varepsilon_i(x)),$$
$$f_x(1) = f(x), \qquad F_x(i) = F(\varepsilon_i(x)),$$

we have Cesàro's general inversion which thus appears as a special case of (12.6).

We shall next indicate how $\mathfrak{C}$, $\mathfrak{E}_r$ combined with an ingenious use of infinite series due to Hermite (*Acta Mathematica*, vol. 5, pp. 297—330; *Journal für Mathematik*, vol. 100, pp. 51—65, and several letters in the Correspondence with Stieltjes), may be applied to functions of the greatest integer $[x] \leq x$. By the usual convention $[x] = 0$ when x is negative. Although it is not necessary in what follows to use infinite series we shall do so for the reasons stated in the Introduction, also because some of the most interesting formulas in the literature of $[x]$ (those relating to the class number,) were first found thus by Hermite, and his method is by no means yet exhausted. A reference to his use of series will show that they suggest transformations which would be unlikely to arise from elementary methods. Hermite ignored all questions of convergence in his memoirs; the justification (if any be needed) of this procedure is contained in $\mathfrak{C}$ as developed in Chapter I. All series are to be considered as the C associated functions of the matrices of their coefficients.

Hermite's fundamental remark is that if

$$F(x) = \sum_0^\infty f(n) x^n,$$

then

$$(12.9)\quad F(x^q)/(1-x) = \sum_0^\infty \{f(0)+f(1)+\cdots+f([n/q])\} x^n,$$

which is obvious on expanding $(1-x)^{-1}$ and collecting the coefficient of x^n. We shall write $\int f(n)$ for the *summatory function of* $f(n)$ *taken between the limits* 1, n, that is

$$\int f(n) = \sum_{a=1}^{n} f(a),$$

and as before, if f, g are in $\mathfrak{E}_r$, fg is their E product, so that

$$fg(n) = \sum f(d)\, g(\delta)$$

extended over all pairs d, δ of conjugate divisors of n. Hence in particular

$$u_0 f(n) = \sum f(d),$$

where $u_r(n) \equiv n^r$, as already defined in § 11, and hence if $F'(x) \equiv F(x) - f(0)$,

$$F'(x^a)/(1-x) = \sum_{n=1}^{\infty} x^n \int f([n/a]). \tag{12.10}$$

Taking $f = u_0$ in the last we have Hermite's generating identity for $[n/a]$,

$$\frac{1}{1-x} \cdot \frac{x^a}{1-x^a} = \sum_{n=1}^{\infty} x^n [n/a]. \tag{12.11}$$

Again, at once from the definitions

$$\sum_{a=1}^{\infty} g(a)\ F'(x^a) = \sum_{n=1}^{\infty} x^n gf(n), \tag{12.12}$$

and therefore

$$\frac{1}{1-x} \sum_{a=1}^{\infty} g(a)\ F'(x^a) = \sum_{n=1}^{\infty} x^n \int gf(n). \tag{12.13}$$

Multiply (12.10) throughout by $g(a)$, sum for $a = 1, \cdots, \infty$, and compare with (12.13). Then, since $gf = fg$ we have

$$\sum_{a=1}^{n} g(a) \int f([n/a]) = \sum_{a=1}^{n} f(a) \int g([n/a]), \tag{12.14}$$

of which there is the useful special case obtained by taking $g \equiv u_0$,

$$\sum_{a=1}^{n} \int f([n/a]) = \sum_{a=1}^{n} [n/a] f(a). \tag{12.15}$$

The last was first given by Liouville and Dirichlet. In the derivation of (12.14) we get incidentally

$$\int fg(n) = \sum_{a=1}^{n} g(a) \int f([n/a]), \tag{12.16}$$

whence we have the useful known theorem

$$\int u_0 f(n) = \sum_{a=1}^{n} [n/a] f(a) = \sum_{a=1}^{n} \int f([n/a]). \tag{12.17}$$

From the inversion (12.6) we see that if

$$H(n) = \sum_{a=1}^{\infty} h(na)\, g(a),$$

then

$$h(1) = \sum_{n=1}^{\infty} g_1(n)\, H(n),$$

where $gg_1 = \eta$, and hence in particular if either $h(n)$ or $H(n)$ vanishes when $n \geqq N$,

$$h(1) = \sum_{n=1}^{N} g(n)\, H(n).$$

Applying this to (12.16) we replace n therein by $[x/n]$, take

$$H(n) = \sum gf([x/n]), \quad \sum([x/n]) = h(n), \quad [x/n] = N,$$

and get as the inversion of (12.16),

$$\sum f(n) = \sum_{a=1}^{n} g_1(a)\, gf([n/a]) \qquad (gg_1 = \eta), \tag{12.18}$$

on replacing $[x]$ by n. Hence the inversion of (12.17) is

$$\sum f(n) = \sum_{a=1}^{n} \mu(a) \sum u_0 f([n/a]), \tag{12.19}$$

since $\mu u_0 = \eta$. Note that (12.18) is a *pair* of inversions, since f, g, g_1 may be replaced by g, f, f_1 respectively.

We shall next give enough examples to show how the formulas (12.14) (12.19) are applied in connection with factorizations in $\mathfrak{E}_r$ as in § 11. In the derivation of (12.14)–(12.19), all of which can be proved almost by inspection, we made only a slight use of Hermite's device, but enough has been given to suggest its utility, for example when applied to the series for theta quotients. The multiplication by the series for $(1-x)^{-1}$ is equivalent to a summation (arithmetical integration); the change of x to x^a in the function to be thus integrated introduces the greatest integer function.

For variety we shall give some examples concerning elements of $\mathfrak{E}_r$ other than those already used in §§ 11–12. Let $\sigma_r(n)$ = the sum of the rth powers of all divisors of n, $\sigma_1(n) \equiv \sigma(n)$, $\sigma_0(n) \equiv \nu(n)$; $\varphi_r(n)$ = the rth Jordan totient of n, $\varphi_1(n) \equiv \varphi(n)$, and $\varphi_r(n)$ = the number of integers $\leq n^r$ that are divisible by the rth power of no prime divisor of n (this is only one of several verbal definitions of the function); $\nu_r(n)$ = the number of divisors of n that are rth powers, $\nu_1(n) \equiv \nu(n)$; $\mu_r(n) = 0$ if n is divisible by an rth power other than unity, $r > 1$, and in every other case the value of the function is 1;

$$\gamma_r(n) = \quad 1 \text{ if } n = n_1^r n_2,\ r > 0, \text{ and } n_2 = 1, \text{ or } \mu(n_2) = 1,$$
$$\gamma_r(n) = -1 \text{ if } n = n_1^r n_2,\ r \geq 0, \text{ and } \mu(n_2) = -1,$$

$\gamma_r(n) = 0$ in all other cases, so that $\mu_r \gamma_r = \eta$ (= the unity in $\mathfrak{E}_r$), and $\gamma_2 = \pi$. The reciprocal of φ_r is ψ_r defined by

$$\varphi_r(n) = n^r\left(1-\frac{1}{p^r}\right)\cdots\left(1-\frac{1}{q^r}\right),\quad \psi_r(n) = (1-p^r)\cdots(1-q^r),$$

where $p, \cdots, q$ are all the different prime divisors of n. In the following examples we shall assume such resolutions in $\mathfrak{E}_r$ as are necessary; all are found immediately from the generators as in § 11. Thus, for example, u_0, μ are reciprocals, so that $u_0\mu = \eta$; also $\mu u_r = \varphi_r$, etc. To simplify the printing we omit all limits from the summation signs, understanding always that $\sum$ refers to a, and continues so long as all arguments of functions in the summands are integers > 0; n in the examples is an arbitrary constant integer > 0. Under the $\int$ sign the implied sum is with respect to $n = 1, 2, \cdots, n$, as above.

From (12.17) and its inverse (12.19) we get, among many others for the functions defined, pairs of inverse relations as follows. Take $f = u_0$; then $u_0 f = u_0^2 = \nu$, $\int u_0(n) = u_1$; hence

$$\int \nu(n) = \sum [n/a], \qquad n = \sum \mu(a) \int \nu([n/a]).$$

Similarly the choice $f = \varphi_r$ gives the pair

$$\int n^r = \sum [n/a]\varphi_r(a) = \int \varphi_r([n/a]),$$

$$\int \varphi_r(n) = \sum (1^r + 2^r + \cdots + [n/a]^r)\mu(a);$$

taking $f = \pi$ we have $u_0 f = k_2$, and hence the pair of inverses

$$[n^{1/2}] = \sum [n/a]\pi(a) = \sum \int \pi([n/a]),$$

$$\int \pi(n) = \sum [(n/a)^{1/2}]\mu(a).$$

Let $S_{r,s}(n) =$ the sum of the sth powers of all divisors of n that are rth powers. Then the choice $f(n) = n^s k_r(n)$ gives

$$\int S_{r,s}(n) = \sum [n/a] a^s k_r(a) = \sum [n/a^r] a^{sr},$$

which, for $s = 1$ is a formula due to Lipschitz,

$$\int S_{r,1}(n) = \sum [n/a^r] a^r.$$

The inverses are uninteresting. Combining the results of taking $f = \pi$, $f = \gamma_r$, $f = k_r$ successively we find the curious result

$$\sum \mu(a) \int \nu_r([n^r/a]) = \sum \mu(a) \int \nu([n/a]) = \sum \int \pi([n^2/a]).$$

These may be continued indefinitely.

From (12.16) and its inverse (12.18) we write down the following examples. Take $g = \psi_r, f = u_r$. Then $gf = u_0$; and the reciprocal of u_r is $|u_r \mu|$, that of ψ_r is φ_r. Hence

$$n = \sum (1^r + 2^r + \cdots + [n/a]^r)\psi_r(a),$$

and this gives the pair of inverses

$$\int n^r = \sum [n/a]\varphi_r(a), \qquad \int \psi_r(n) = \sum [n/a] a^r \mu(a).$$

The choice $f = u_0$, $g = |\mu^2|$ and the factorization $|\mu^2|\, u_0 = \theta$ in $\mathfrak{E}_r$ give the following, due to Dirichlet,

$$\int \theta(n) = \sum \mu^2(a)\,[n/a],$$

and hence, since $|\mu^2|\pi = \eta$, we have the inverses

$$n = \sum \pi(a) \int \theta([n/a]) = \sum \theta(a) \int \pi([n/a]),$$
$$\int \mu^2(n) = \sum \mu(a) \int \theta([n/a]).$$

Taking $f = |u_1 k_r|$, $g = |u_1 \mu_r|$ we get

$$n(n+1)/2 = \sum \{1^r + 2^r + \cdots + [(n/a)^{1/r}]^r\}\, a\mu_r(a),$$

where the absence of r on the left is noticeable, and this gives the inverse (we omit one)

$$2\sum a\mu_r(a) = \sum [n/a^r]\,(1+[n/a^r])\,a^r\mu(a).$$

The choice $f = u_1$, $g = |u_1\mu|$ gives $fg = \eta$, and hence

$$2 = \sum [n/a]\,(1+[n/a])\,a\mu(a)$$

which is its own inverses.

By a slight variation of the extremely simple technique we write down the following in conclusion:

$$\begin{aligned}
n(n+1) &= 2\sum \{\varphi([n/a]) + [n/a]\,\varphi(a-1)\},\\
1 &= \sum \{\mu([n/a]) + [n/a]\,\mu(a-1)\},\\
[n^{1/2}] &= \sum \{\pi([n/a]) + [n/a]\,\pi(a-1)\},\\
\int \sigma_r(n) &= \sum [n/a]\,\{[n/a]^{r-1} + (a-1)^r\},\\
\int \lambda(n) &= \sum P([n/a]),
\end{aligned}$$

where $P(n) =$ the number of primes $\leqq n$. As a numerical verification we take $n = 6$ in the last, getting on the left $1+2+2+2+2+3$ and on the right $4+3+2+1+1+1$.

Formulas such as those in the examples have frequently been used as the point of departure for obtaining mean

values of arithmetial functions. Their interest here is that they may be constructed at will by processes which are abstractly identical with the simplest multiplications and divisions in $\mathfrak{A}$.

EXTENSIONS AND FURTHER INSTANCES OF $\mathfrak{E}$, §§ 13–14

13. Extension of $\mathfrak{E}$ to sets of elements. For simplicity we consider only the case where the arguments of the functions are integers, but the whole of $\mathfrak{E}$ may be reconstructed on similar lines. There are no instances in the literature of the type of relations between integers to which these extensions give rise.

Call $f \equiv f(x_1, \cdots, x_r)$ a *numerical function* if f for each set of integral values, all different from zero, of the x_i takes a single finite value, and if further $f(1, 1, \cdots, 1) \neq 0$. Let $\sum$ refer to all integers $n_{ji}\,(j = 1, \cdots, t;\ i = 1, \cdots, r)$ which, for constant integers $n_i\,(i = 1, \cdots, r)$, each $\geqq 1$, satisfy

$$n_i = n_{1i}\, n_{2i} \cdots n_{ti} \qquad (i = 1, \cdots, r),$$

and let

$$f_j \equiv f_j(x_1, \cdots, x_r) \qquad (j = 1, \cdots, t)$$

be t numerical functions. Then the *t-fold D product* $f_1\, f_2 \cdots f_t$ with the *matric argument* $N_r \equiv (n_1, n_2, \cdots, n_r)$ is defined as

$$f_1\, f_2 \cdots f_t = \sum \left[\prod_{j=1}^{t} f_j(n_{j1}, n_{j2}, \cdots, n_{jr}) \right].$$

As in $\mathfrak{E}_r$ we may omit reference to N_r.

The unity of this multiplication is easily seen to be the numerical function

$$u \equiv u(x_1, \cdots, x_r)$$

defined by the properties $u = 1$ when $x_j = 1\,(j = 1, \cdots, r)$, $u = 0$ otherwise. Evidently $uf = f$, where f is any numerical function (of r arguments). The zero of multiplication is the function w which vanishes for all matric arguments, $wf = w$.

Precisely as in $\mathfrak{E}$ or $\mathfrak{E}_r$ it can be shown that $f \neq w$ has a unique reciprocal f', that is, the equation $ff' = u$ has

one and only one solution (numerical function of r arguments) f'. Hence multiplication has a unique inverse and is abstractly identical with multiplication in $\mathfrak{A}$.

Let ζ be the numerical function which takes the value 1 for all values of its matric argument N_r, and let $\zeta\zeta' = u$. Then it follows easily that $\zeta'(n_1, \cdots, n_r) = 0$ if the $n_j (j = 1, \cdots, r)$ are not all simple, and in the contrary case the value is 1 or -1 according as an even or an odd number of the n_j have odd manifoldness (see § 11). Hence each of ζ, ζ' is a solution τ of

$$\tau(n_1, n_2, \cdots, n_r) = \tau(n_1)\,\tau(n_2)\cdots\tau(n_r),$$

and we see that if f, g are any numerical functions (of r arguments),

$$g = \zeta f \,.\supset.\, f = \zeta' g,$$

which is a generalization of Dedekind's inversion ($r = 1$). Again, precisely as in $\mathfrak{E}_r$,

$$fg = h \,.\supset.\, g = hf' \quad and \quad f = hg',$$
$$af = bg \quad and \quad ah = bk \,.\supset.\, fk = gh,$$

and so on. The abstract identity with $\mathfrak{A}$ gives, as in $\mathfrak{E}_r$, an infinity of such relations. The functional powers f^g also exist as in $\mathfrak{E}_r$.

There is a theory of associated functions here as in $\mathfrak{D}$, but not one of generators—as in $\mathfrak{E}_r$. Finally, as already mentioned, the extension can be readily made to functions of r arguments belonging to r distinct semigroups.

14. Other instances of $\mathfrak{E}$. From the manner in which $\mathfrak{E}$ was constructed it is clear that the integer n in (3.4) may be replaced by the particular general element n of any variety $\mathfrak{V}$ in which the fundamental theorem of arithmetic holds, provided $\alpha, \beta, \cdots, \gamma$ be replaced by the prime factors of n in $\mathfrak{V}$. For instance, $n, a, \beta, \cdots, \gamma$ may denote ideals in a given algebraic number field, n being considered principal (corresponding to a given algebraic integer) when $\alpha, \beta, \cdots, \gamma$

become the distinct prime ideal factors (not necessarily principal) of n. In any instance the uniform functions $f_a(x_a), \cdots$ on which $\mathfrak{E}$ is constructed can be chosen only such that addition and subtraction are significant for them. Thus, in the case of ideals we might choose for $f_a(x_a)$ the norm of α^a. The further development in any instance proceeds precisely as in $\mathfrak{E}$. It is immaterial according to what law the elements x_n (n in $\mathfrak{B}$) are arranged into derived matrices, provided the first element be that corresponding to the unity in $\mathfrak{B}$, as we work only with generators and the general elements of the matrices. It is sufficient to know that the x_n for $\mathfrak{B}$ can be placed in (1, 1) correspondence with those for $\mathfrak{E}$. The last follows since the elements of $\mathfrak{B}$ are denumerable, by our assumptions in Chapter I concerning arithmetic.

APPLICATIONS OF $\mathfrak{C}$ TO THE ALGEBRA OF SEQUENCES, §§ 15–17

15. Blissard's umbrae. The applications in question are made by means of the variety $\mathfrak{B}$ of $\mathfrak{C}$ described in Chapter I § 22. As the subject is very extensive, and its applications numerous, we can give only the briefest outline. A systematic use of the algebra sketched here greatly abridges the computations necessary in the algebra of sequences of functions or numbers and, what is more significant, suggests many interesting extensions or generalizations of well known theories—for example those of the several kinds of Bernoullian functions in existence (including their usual generalizations to functions of several variables), the like for the Eulerian functions, and the essential generalizations of all these which result when the numbers of Bernoulli and Euler are replaced by the polynomials occurring as coefficients in the power series expansions of elliptic functions. The algebra has in fact immediate and fruitful application to any functions containing in their definition an arbitrary integer.

The consequences of representing the entire class of elements c_n ($n = 0, 1, \cdots$) of $\mathfrak{A}$ by the single letter or *umbra* c were first developed by Blissard in a series of papers on the *Theory*

of Generic Equations in vols. 4 6 of the *Quarterly Journal*. Essentially the same theory, with less detail, was stated about 15 years later by Lucas, who also gave a short account of it in chapters X XIII of his *Théorie des Nombres* (1891). The theory of Blissard's method can be carried much beyond its current state; it can indeed be developed in complete isomorphism with $\mathfrak{A}$. The extension of the method by the introduction of umbral division, umbral differentiation and integration, the umbral circular functions, etc., lead to particularly interesting consequences. As Blissard's work seems to have been overlooked by many who attribute its simple and ingenious processes to later writers, I have designated the algebra based on it by $\mathfrak{B}$ to recall the name of its originator. In a certain sense $\mathfrak{B}$ includes $\mathfrak{A}$. This will appear so far as multiplication is concerned presently; I shall not take the space to consider true umbral addition and division (not discussed by Blissard or Lucas), which completes the inclusion. If $(c_0, c_1, \cdots)$ is any matrix in $\mathfrak{A}$ we shall denote this matrix by c, and call c the *umbra* of the matrix; c is not an element of $\mathfrak{A}$. The interpretation of the umbral power c^n is that *this power represents the n th element* c_n *of the matrix* $(c_0, c_1 \cdots)$ *of which c is the umbra;* c^0 *represents* c_0. If c is any umbra we shall write $c^n = c_n$ $(n = 0, 1, \cdots)$. In dealing with several umbrae it is occasionally necessary to give them suffixes. Thus, for example, the umbra of the C matrix $(b_{r0}, b_{r1}, \cdots, b_{rn}, \cdots)$ in $\mathfrak{A}$ may be designated by b_r, and we have $b_r^n = b_{rn}$ $(n = 0, 1, \cdots)$. Umbrae are combined in $\mathfrak{C}$ or $\mathfrak{B}$ according to the following fundamental rules.

Umbral powers c^n, c^m, $\cdots$ (m, n integers $\geqq 0$) occurring in computations are manipulated as if they were scalars (= elements of $\mathfrak{A}$) with the three following restrictions: (1) zeroth powers a^0, b^0, $\cdots$ of umbrae a, b, $\cdots$ must always be indicated explicitly and are not to be replaced by the unity 1 of $\mathfrak{A}$; (2) if in any linear function of umbrae with raised suffixes a given umbra occurs precisely s times, it is to be replaced by s distinct umbrae until after the completion of all operations as in $\mathfrak{A}$, when (3) all exponents (raised suffixes) of

umbrae are degraded to suffixes. Umbrae are equal only when the matrices of which they are the umbrae are equal.

To the absolute product $|a'b|$ of

$$a' \equiv (1, a, a^2, \cdots), \qquad b \equiv (b_0, b_1, b_2, \cdots),$$

where $a^n, b_n (n = 0, 1, \cdots)$ are scalars, we assign the umbra $a'b$. Hence $a'b$ is the umbra of $(b_0, ab_1, a^2 b_2, \cdots)$, since a^0 is a scalar and hence $= 1$ (the unity in $\mathfrak{A}$).

16. Umbral $\mathfrak{T}$. The $\mathfrak{T}$ to which we refer is that of Chapter II, § 7. Let $a, b, \cdots, c$ be k umbrae, $x, y, \cdots, z$ scalars, and $n \geqq 0$ an integer. Then by definition

$$(xa + yb + \cdots + zc)^n = \sum \frac{n!}{\alpha!\,\beta! \cdots \gamma!} x^\alpha y^\beta \cdots z^\gamma\, a_\alpha b_\beta \cdots c_\gamma,$$

where $\sum$ refers to all sets of k integers each $\geqq 0$ whose sum is n. Hence (see chapter I § 22), if t is also scalar,

$$\exp xat \exp ybt \cdots \exp zct = \exp (xa + yb + \cdots + zc)t.$$

Hence if i as in $\mathfrak{F}_c$ is the imaginary unit, the umbral sine and cosine are defined by

$$2i \sin at = \exp iat - \exp(-iat),$$
$$2 \cos at = \exp iat + \exp(-iat);$$

whence

$$\sin at = \sum_0^\infty \frac{(-1)^n t^{2n+1}}{(2n+1)!} a_{2n+1}, \quad \cos at = \sum_0^\infty \frac{(-1)^n t^{2n}}{(2n)!} a_{2n},$$

and with an obvious meaning for the umbral derivative

$$\frac{d}{da} \sin at = t \cos at, \qquad \frac{d}{da} \cos at = -t \sin at,$$

also

$$\frac{d}{dt} \sin at = a \cos at, \qquad \frac{d}{dt} \cos at = -a \sin at,$$

in the last two of which the indicated multiplication by a is to be performed (see § 15) before exponents are degraded; in the first pair of derivatives the differentiations are per-

formed upon the series for $\sin at$, $\cos at$ in the forms with raised suffixes.

If in the above umbral $(xa+yb+\cdots+zc)^n$ we *interpret* $a, b, \cdots, c$ as scalars, the expansion becomes the multinomial theorem in $\mathfrak{A}$, and similarly, mutatis mutandis, for the umbral exponentials and circular functions. We shall refer to this interpretation as the *scalar instance* of the umbral functions, and similarly for scalar instances of umbral identities. It is clear, that the scalar instance of an umbral identity is an identity in $\mathfrak{A}$. Hence any umbral identity can be read in either of two ways, namely as identity between scalars or as one between umbrae. The second is the more inclusive. For example the umbral expansion of $(a+b-a)^2$ can be written

$$\begin{aligned} a^2(b-a)^0+2a^1(b-a)^1+a^0(b-a)^2 \\ = a^2b^0a^0+2a^1(b^1a^0-b^0a^1) \quad +a^0(b^2a^0-2b^1a^1+b^0a^2) \\ = a_2b_0 \quad +(2a_1b_1-2a_2b_0) \quad + \quad (a_0b_2-2a_1b_1+a_2b_0), \end{aligned}$$

which reduces to a_0b_2. Hence $(a+b-a)^2 = a^0b^2$ either umbrally or in $\mathfrak{A}$, since in $\mathfrak{A}$ we have $a^0 = 1$.

For $n \geq 0$ an integer we define as the simplest instances of functions to be generalized presently

$$\varphi_n(a,b) \equiv (a+b)^n+(a-b)^n, \quad \psi_n(a,b) \equiv (a+b)^n-(a-b)^n,$$

where a, b are umbrae, and hence if t is scalar as before

$$\begin{aligned} 2\cos at\cos bt &= \cos(a+b)t+\cos(a-b)t = \quad \cos\varphi(a,b)t, \\ 2\cos at\sin bt &= \sin(a+b)t-\sin(a-b)t = \quad \sin\psi(a,b)t, \\ 2\sin at\cos bt &= \sin(a+b)t+\sin(a-b)t = \quad \sin\varphi(a,b)t, \\ 2\sin at\sin bt &= \cos(a-b)t-\cos(a+b)t = -\cos\psi(a,b)t, \end{aligned}$$

in abstract identity with $\mathfrak{T}$. The first, for example, states that the coefficient of $(-1)^n t^{2n}/(2n)!$ in the product

$$2\sum_0^\infty \frac{(-1)^n t^{2n}}{(2n)!}a_{2n}\sum_0^\infty \frac{(-1)^n t^{2n}}{(2n)!}b_{2n}$$

is

$$(a+b)^{2n}+(a-b)^{2n} = 2\sum_{r=0}^{n}\binom{2n}{2r} a_{2n-2r}\, b_{2r}.$$

Since we are operating in $\mathfrak{C}$ or $\mathfrak{B}$ convergence is irrelevant; the series are merely those associated with the matrices of their coefficients as explained in chapter I.

It now follows that, precisely as in obtaining the $\mathfrak{P}$ isomorph of $\mathfrak{T}$ in Chapter II §§ 7–9, *there is a complete umbral* $\mathfrak{T}$. say $\mathfrak{T}_u$. In this the most useful formulas are the generalizations of the above to any number of umbral arguments and the abstractly identical equivalents in $\mathfrak{T}_u$ of the addition theorems in $\mathfrak{T}$.

The formulas for composition and decomposition in $\mathfrak{T}$ are the scalar instances of an important set of formulas in $\mathfrak{T}_u$. whose application will be pointed out after we have indicated their nature. Let the $u_j, v_j, u'_j, v'_j, \cdots (j = 1, 2, \cdots)$ denote umbrae, so that, for example, $u_j^n = u_{jn}$ $(n = 0, 1, \cdots)$, and in the scalar instance, $u_{jn} = u_j^n$. where u_j is interpreted as an element of $\mathfrak{A}$. From these umbrae we can now form D matrices, precisely as in the scalar instance. Write

$$U_r \equiv (u_1, u_2, \cdots, u_r), \qquad V_s \equiv (v_1, v_2, \cdots, v_s),$$
$$U'_p \equiv (u'_1, u'_2, \cdots, u'_p), \qquad V'_q \equiv (v'_1, v'_2, \cdots, v'_q), \cdots.$$

and as in previous chapters indicate conjunction by plus signs. thus $U_r + V_s$. The particular order chosen as normal for the u_j, v_k in the conjoint is immaterial in what follows (as will appear presently); for definiteness that order may be taken as normal in which the v's follow the u's. and accented letters follow unaccented. Thus

$$U_r + V_s = (u_1, u_2, \cdots, u_r, v_1, v_2, \cdots, v_s),$$
$$U_r + U'_p = (u_1, u_2, \cdots, u_r, u'_1, u'_2, \cdots, u'_p).$$

Each of e_j, ε_j $(j = 1, 2, \cdots)$ as in $\mathfrak{P}$ denotes a definite one of $1, -1$, and $\sum$ refers to all possible sets of values of the e's and ε's occurring in the arguments of the summand; the functions φ, ψ, χ are then defined for $n = 0, 1, \cdots$ by

$$\varphi_n(U_r) \equiv \sum (u_1 + e_2 u_2 + e_3 u_3 + \cdots + e_r u_r)^n.$$
$$\psi_n(V_s) \equiv \sum \varepsilon_2 \varepsilon_3 \cdots \varepsilon_s (v_1 + \varepsilon_2 v_2 + \cdots + \varepsilon_s v_s)^n,$$
$$\chi_n(U_r; V_s) \equiv \sum \varepsilon_1 \varepsilon_2 \cdots \varepsilon_s (u_1 + e_2 u_2 + \cdots + e_r u_r + \varepsilon_1 v_1 + \varepsilon_2 v_2 + \cdots + \varepsilon_s v_s)^n.$$

Hence, t being scalar, we have from chapter II § 10,

$$2^{r-1} \prod_{j=1}^{r}{}' \cos u_j t = \cos \varphi(U_r) t,$$
$$2^{2s-1} (-1)^s \prod_{j=1}^{2s} \sin v_j t = \cos \psi(V_{2s}) t,$$
$$2^{2s} (-1)^s \prod_{j=1}^{2s+1} \sin v_j t = \sin \psi(V_{2s+1}) t,$$
$$2^{r+2s-1} (-1)^s \prod_{j=1}^{r} \cos u_j t \cdot \prod_{k=1}^{2s} \sin v_k t = \cos \chi(U_r; V_{2s}) t,$$
$$2^{r+2s} (-1)^s \prod_{j=1}^{r} \cos u_j t \cdot \prod_{k=1}^{2s+1} \sin v_k t = \sin \chi(U_r; V_{2s+1}) t.$$

The φ_n, ψ_n, χ_n are therefore instances of parity functions, and the respective parities of $\varphi_{2n}(U_r)$, $\psi_{2n}(V_{2s})$, $\psi_{2n+1}(V_{2s+1})$, $\chi_{2n}(U_r; V_{2s})$, $\chi_{2n+1}(U_r; V_{2s+1})$ are $p(U_r|)$, $p(V_{2s}|)$, $p(|V_{2s+1})$, $p(U_r, V_{2s}|)$, $p(U_r|V_{2s+1})$.

If now we multiply together corresponding members of any pair of such identities and use the above to reduce the results to the same respective forms, we find six addition theorems for the φ, ψ, χ functions, of which we shall write only two,

$$\varphi_{2n}(U_r + U'_p) = \varphi_{2n}(\varphi(U_r), \varphi(U'_p)),$$
$$\chi_{2n+1}(U_r + U'_p; V_{2s} + V'_{2q+1}) = \psi_{2n+1}(\chi(U_r; V_{2s}), \chi(U'_p; V'_{2q+1})).$$

Similarly, if each umbra in U_r be replaced by the sum of two others, for example $u = v + w$, so that $u^n = (v + w)^n$ $(n = 0, 1, \cdots)$, we find in the same way a second kind of addition theorem, of which a simple instance is

$$2\varphi_{2n}(U_r,\ u'+u'') = \varphi_{2n}(U_r,\ u',\ u'') - \chi_{2n}(U_r;\ u',\ u''),$$

where each of u', u'' is an umbra (not a matrix of umbrae). Combining the two kinds we get a third, of which a specimen is

$$\chi_{2n}(u;\ V_{2s+1},\ v) = \varphi_{2n}(u,\ \psi(V_{2s+1},\ v)),$$

where u, v are umbrae. As in $\mathfrak{T}$ there are subtraction theorems, obtained in an obvious way similarly to the above, and by combinations of the resulting formulas with the addition theorems we reach three types of expansion and decomposition formulas in $\mathfrak{T}$ each abstractly identical with the single set in $\mathfrak{T}$.

The simplest application of such formulas is to the functional generalization of recurrence relations for sequences of numbers or functions. Let $f(t)$ be a function in $\mathfrak{A}$ of the type

$$f(t) = c_0 + c_1 t + c_2 t^2 + \cdots,$$

where the series may terminate. If in the instances $\mathfrak{F}_j$ $(j = r, \cdots)$ of $\mathfrak{A}$ the series does not terminate it is usually assumed that it is convergent for the values of t considered; if the series is divergent it is interpreted as the associated function of $(c_0, c_1, \cdots)$. Then, the $\sum$ referring as before to the e's, and k being an arbitrary scalar, we have

$$f(t + k\varphi(U_r)) = \sum f(t + k(u_1 + e_2 u_2 + \cdots + e_r u_r)),$$

with analogous formulas (involving products of e's or ε's as coefficients on the right) for ψ, χ. Let each of ι, λ, μ, $\cdots$, ν denote a definite one of φ, ψ, χ for given arguments U_a, V_b, $\cdots$. Referring to the original definitions of $\varphi_n(U_r)$, $\psi_n(V_s)$, $\chi_n(U_r; V_s)$ we write now

$$\begin{aligned} T\varphi(U_r) &= u_1 + e_2 u_2 + \cdots + e_r u_r, \\ T\varphi(V_r) &= v_1 + \varepsilon_2 v_2 + \cdots + \varepsilon_s v_s, \\ T\varphi(U_r; V_s) &= T\varphi(U_r) + \varepsilon_1 v_1 + \varepsilon_2 v_2 + \cdots + \varepsilon_s v_s, \end{aligned}$$

or understanding in any case U_r, V_s, simply $T\varphi$ for the corresponding sum on the right, and

$$S\varphi(U_r) = 1, \quad S\varphi(V_r) = e_2 e_3 \cdots e_r, \quad S\varphi(U_r; V_s) = \varepsilon_1 \varepsilon_2 \cdots \varepsilon_s,$$

with similar abbreviations to $S\varphi$. If several $T\varphi$, $S\varphi$ occur in one formula the e's and ε's are to be treated as umbrae; that is, the sets of units pertaining to different functions are to be denoted by distinct sets of letters, thus $e_j, e'_j, \varepsilon_j, \varepsilon'_j, \cdots$ $(j = 1, 2, \cdots)$. This is merely to prevent confusion in assigning to the argument of Σ in the following all possible sets of values of the e's and ε's (each $= \pm 1$). Suppose now that between $\tau, \lambda, \mu, \cdots, \nu$ for the given arguments there is the relation $\tau = \lambda + \mu + \cdots + \nu$. Then, f being as above, we have

$$f(t+\tau) = S(\lambda) S(\mu) \cdots S(\tau) f(t + T(\lambda) + T(\mu) + \cdots + T(\nu)),$$

as is easily seen. This is the prototype of all recurrence formulas for sequences of elements of either type

$$u_0, u_2, u_4, u_6, \cdots, \qquad v_1, v_3, v_5, v_7, \cdots.$$

By the proper change in notation any sequence can be written in either of these forms (with all even or all odd suffixes). If the sequences are given directly in the form $w_0, w_1, w_2, w_3, \cdots$ the exponential theorem (umbral) is used from the beginning, instead of the circular functions, and we reach correspondingly simpler formulas. Thus if $\alpha, \beta, \gamma, \cdots, \delta$ are umbrae such that $\alpha = \beta + \gamma + \cdots + \delta$, then immediately

$$f(t+\alpha) = f(t+\beta+\gamma+\cdots+\delta).$$

It remains to indicate briefly how umbral equalities such as $\tau = \lambda + \mu + \cdots$ or $\alpha = \beta + \gamma + \cdots$ above may be found, and it will be sufficient to take as an illustration the simplest example from functions of a single variable. Let $f(t)$ be an even function of t, and $g(t)$ an odd function in $\mathfrak{F}_c$, both possessing MacLaurin expansions for some $|t|$. Then the expansions may be written

$$f(t) = \cos at, \quad g(t) = \sin bt,$$

where a, b are umbrae. If now we have several such functions and their expansions.

$$h(t) = \cos ct, \qquad k(t) = \sin dt, \cdots$$

their products define further even or odd functions, and we have for example

$$2f(t)h(t) = l(t) = \cos et = \cos \varphi(a, c)t$$
$$2g(t)k(t) = m(t) = -\cos rt = -\cos \psi(b, d)t,$$

where we have regarded the products fh, gk as defining new umbrae e, r, and we have

$$e_{2n} = \varphi_{2n}(a, c), \qquad r_{2n} = \psi_{2n}(b, d) \qquad (n = 0, 1, \cdots).$$

Again, since $f(t)$ is even, $a_{2n+1} = 0$ $(n = 0, 1, \cdots)$ and hence $\varphi_{2n+1}(a, c) = 0$. Thus if we define the e's of odd ranks, namely e_{2n+1}, by $e_{2n+1} = \varphi_{2n+1}(a, c)$, we have $e_n = \varphi_n(a, c)$ $(n = 0, 1, \cdots)$, and hence $e = \varphi$. Similarly for products of several factors. A simple example is given by the Euler numbers E_{2n} $(n = 0, 1, \cdots)$, $E_{2n+1} = 0$, defined by $\sec t = \cos Et$. Hence

$$2 = 2\sec t \cos t = 2\cos Et \cos t = \cos \varphi(E, 1)t,$$

and therefore $\varphi(E, 1) = u$, where $u_0 = 2$, $u_n = 0$ $(n > 0)$.

In general the expansions of any set of functions define a unique set of umbrae; by means of the algebraic or analytic properties of the functions, or by merely considering the expansions of their reciprocals, powers, etc., we generate new umbrae and obtain equalities between the new umbrae and the old. Extremely simple equalities such as these frequently appear as the origin or the core of elaborate theories of the algebraic aspects of sequences of functions or numbers, for example those of Bernoulli, Euler, Genocchi, Lucas, and the Legendre and Bessel functions.

The umbral differential calculus can be readily developed from the following definition, abstractly identical with that for the rth derivative of a^n with respect to a in $\mathfrak{F}_c$.

$$D_a^r a_n = \frac{n!}{(n-r)!} a_{n-r}$$

where D_a^r denotes the rth umbral derivative with respect to the umbra a. We have also, writing $D_a = d/da$,

$$\frac{d}{da} f(a+t) = \frac{d}{dt} f(a+t).$$

precisely as in $\mathfrak{F}_c$. The last is a useful formula.

17. Umbral fields. An infinity of fields, regular or irregular, can be devised for the study of special sequences. The interpretations assigned to the four fundamental operations are determined by the sequences concerned and particular relations between them which it is desired to investigate; the flexibility of the method allows it to be bent to any algebraic end. For example, if it be desired to extend to negative ranks $-n$ a sequence of functions or numbers commonly defined only for $n > 0$, the algebra at once provides the generators of the extended sequence in such forms that they are consistent with the initially given functions or numbers. The simplest umbral fields are isomorphic to the umbral exponential functions. Two examples will be sufficient. Latin letters $a, b, \cdots, c$ denote umbrae, Greek $\alpha, \beta, \cdots, \gamma$ scalars.

We have defined αa to be the umbra of $(a_0, \alpha a_1, \alpha^2 a_2, \cdots, \alpha^n a_n, \cdots)$. We designate the umbra of $(\alpha a_0, \alpha a_1, \cdots, \alpha a_n, \cdots)$ by the new symbol $(\alpha \cdot a)$, $= (a \cdot \alpha)$. From the set of all $(\alpha \cdot a)$ generated as α runs through all elements of $\mathfrak{A}$ and a through all umbrae of matrices in $\mathfrak{A}$, we shall construct an irregular field $\mathfrak{J}\mathfrak{U}$. The sum in $\mathfrak{J}\mathfrak{U}$ of any two elements $(\alpha \cdot a)$, $(\beta \cdot b)$ of $\mathfrak{J}\mathfrak{U}$ will be written $(\alpha \cdot a) \cdot + \cdot (\beta \cdot b)$, and their product $(\alpha \cdot a) \cdot (\beta \cdot b)$, both of which are to be so defined that they satisfy the postulates of an irregular field

as stated in Chapter I § 3. This may be done in several ways. The following is given in some detail as it is typical of all cases. We first, as a preliminary survey to determine the interpretations of addition and multiplication, transpose additive and multiplicative properties of the functions discussed (here umbral exponentials) into terms of umbrae alone. Having seen what interpretations are sufficient we then suppress all mention of the exponentials and construct the field ab initio, verifying independently from the definitions given by the survey that these do indeed satisfy the required postulates.

From the definition of $(\alpha \cdot a)$ as the umbra of $(\alpha a_0, \cdots, \alpha a_n, \cdots)$, it follows that

$$\exp\,(\alpha \cdot a)t = \sum \alpha a_n t^n/n! :\supset: (\alpha \cdot a)^n = \alpha a_n.$$

Now $\exp(\alpha \cdot a)t$ is in $\mathfrak{A}$, being an associated function of the matrix whose umbra is $(\alpha \cdot a)$. Hence, if $\varphi(\alpha, \beta, \cdots, \gamma)$ is a function in $\mathfrak{A}$, so also is

$$\varphi(\exp(\alpha \cdot a)t,\ \exp(\beta \cdot b)t, \cdots, \exp(\gamma \cdot c)t).$$

From the definition of $(\alpha \cdot a)$ we have

$$\exp at = \exp(\alpha \cdot a)t, \qquad (1 \cdot a) = a.$$

Take now $\varphi(\alpha, \beta) = \alpha + \beta$. Then it is suggested thus that we define the sum in $\mathfrak{J}\mathfrak{U}$ of $(\alpha \cdot a)$, $(\beta \cdot b)$ through

$$\alpha \exp at + \beta \exp bt = \exp((\alpha \cdot a) \cdot + \cdot (\beta \cdot b))t.$$

which states that $(\alpha \cdot a) \cdot + \cdot (\beta \cdot b)$ in $\mathfrak{J}\mathfrak{U}$ is the umbra of the matrix whose nth element is $a\alpha_n + b\beta_n$ in $\mathfrak{A}$, and hence

$$((\alpha \cdot a) \cdot + \cdot (\beta \cdot b))^n = \alpha a_n + \beta b_n.$$

Similarly, taking $\varphi(\alpha, \beta) = \alpha \cdot \beta$ in $\mathfrak{A}$, we may define multiplication in $\mathfrak{J}\mathfrak{U}$ through

$$\alpha \exp at \cdot \beta \exp bt = \exp((\alpha \cdot a) \cdot (\beta \cdot b))t,$$

the indicated product on the left being in $\mathfrak{A}$, so that

$$((\alpha \cdot a) \cdot (\beta \cdot b))^n = \alpha\beta(a+b)^n = \alpha\beta \sum_{j=0}^{n} \binom{n}{j} a_{n-j} b_j.$$

Thus we may take as the product $(\alpha \cdot a) \cdot (\beta \cdot b)$ in $\mathfrak{J}\mathfrak{U}$ of $(\alpha \cdot a)$, $(\beta \cdot b)$ the umbra of the matrix whose nth element is the element $\alpha\beta(a+b)^n$ of $\mathfrak{A}$.

In the same way the unity $(1 \cdot u) = u$ and the zero $(1 \cdot z) = z$ in $\mathfrak{J}\mathfrak{U}$ are indicated at once: it is sufficient to take $u_0 = 1$ (the unity in $\mathfrak{A}$), $u_n = 0\ (n > 0)$, and $z_n = 0\ (n = 0, 1, \cdots)$. Further $(\alpha \cdot a)$ is regular if and only if $\alpha a_0 \neq 0$, and if $(\alpha \cdot a)$, $(\beta \cdot b)$ are given, and $(\alpha \cdot a)$ is regular, then there exists a unique element $(\gamma \cdot c)$ in $\mathfrak{J}\mathfrak{U}$, called the quotient of $(\beta \cdot b)$ by $(\alpha \cdot a)$, such that $(\alpha \cdot a) \cdot (\gamma \cdot c) = (\beta \cdot b)$, for the last is equivalent to

$$\alpha\gamma \sum_{j=0}^{n} \binom{n}{j} a_{n-j} c_j = \beta b_n \qquad (n = 0, 1, \cdots),$$

which uniquely determine $\gamma c_n\ (n = 0, 1, \cdots)$ if and only if $\alpha a_0 \neq 0$.

Having thus foreseen a possible set of interpretations for the four fundamental operations in $\mathfrak{J}\mathfrak{U}$ by means of an isomorphism with umbral exponentials, we can discard the latter and construct $\mathfrak{J}\mathfrak{U}$ independently. Formal proofs that the following interpretations are self consistent and an instance of the postulate system for an irregular field are superfluous, as they are implied by the abstract identity with exponentials which we are discarding. It will however be of interest to show how one or two are proved directly from the postulates.

We take as elements of $\mathfrak{J}\mathfrak{U}$ the $(\alpha \cdot a)$, $(\beta \cdot b)$, $\cdots$, $(\gamma \cdot c)$, $\cdots$ as first defined (without reference to exponentials), so that $(\alpha \cdot a)^n = \alpha a_n (n = 0, 1, \cdots)$ and $(\alpha \cdot a) = (\beta \cdot b)$, by the definition of umbral equality, only when $(\alpha \cdot a)^n = (\beta \cdot b)^n$ $(n = 0, 1, \cdots)$. Then $(\alpha \cdot a) \cdot + \cdot (\beta \cdot b)$ is defined as the umbra of the matrix whose nth element is $\alpha a_n + \beta b_n$, and $(\alpha \cdot a) \cdot (\beta \cdot b)$ as the umbra of the matrix whose nth element is $\alpha\beta(a+b)^n$; the zero, unity in $\mathfrak{J}\mathfrak{U}$ are $(1 \cdot u)$, $(1 \cdot z)$ respectively.

as above. With these definitions it is easily shown from first principles that $\mathfrak{J}\mathfrak{U}$ is an instance of $\mathfrak{J}\mathfrak{F}$ in chapter I § 3. For example, the unique negative $(1\cdot z)\cdot -\cdot(\alpha\cdot a)$ of $(\alpha\cdot a)$ is $(-\alpha\cdot a)$, the last being the umbra of the matrix whose nth element is $-\alpha a_n$. Again, if the associative law of multiplication holds, we should have

$$(\alpha\cdot a)\cdot((\beta\cdot b)\cdot(\gamma\cdot c)) = ((\alpha\cdot a)\cdot(\beta\cdot b))\cdot(\gamma\cdot c),$$

and hence

$$(\alpha\cdot a)\cdot(\beta\gamma\cdot bc) = (\alpha\beta\cdot ab)\cdot(\gamma\cdot c),$$

that is, $(\alpha\beta\gamma\cdot abc) = (\alpha\beta\gamma\cdot abc)$, which completes the verification. The distributive law states that

$$(\gamma\cdot c)\cdot((\alpha\cdot a)\cdot+\cdot(\beta\cdot b)) = (\gamma\alpha\cdot ca)\cdot+\cdot(\gamma\beta\cdot cb).$$

Set $(\alpha\cdot a)\cdot+\cdot(\beta\cdot b) \equiv (1\cdot d)$, as obviously is permissible. Then it must be shown that

$$(\gamma\cdot c)\cdot(1\cdot d) = (\gamma\alpha\cdot ca)\cdot+\cdot(\gamma\beta\cdot cb),$$

and therefore

$$[c+((\alpha\cdot a)\cdot+\cdot(\beta\cdot b))]^n = \alpha(c+a)^n+\beta(c+b)^n.$$

The left of this is

$$\sum_{j=0}^{n}\binom{n}{j}c_{n-j}(\alpha a_j+\beta b_j),$$

which is identical with the right, thus verifying the distributive law.

From $\mathfrak{J}\mathfrak{U}$ further irregular fields may be generated. Thus, if θ is a variable in $\mathfrak{A}$, then

$$A_n(\theta,(\alpha\cdot a)) \equiv (\theta+(\alpha\cdot a))^n = \alpha\sum_{j=0}^{n}\binom{n}{j}a_{n-j}\theta^j,$$

defines a matrix of polynomials in $\mathfrak{A}$ whose umbra is $A(\theta,(\alpha\cdot a))$. Call $(\alpha\cdot a)$ the *index* of $A(\theta,(\alpha\cdot a))$, and write

$$(\alpha\cdot a)\cdot+\cdot(\beta\cdot b) \equiv (1\cdot s), \qquad (\alpha\cdot a)\cdot(\beta\cdot b) \equiv (1\cdot p).$$

Then there exists an irregular field $\mathfrak{J}\mathfrak{U}_A$ whose elements are the $A(\theta,(\alpha\cdot a))$, where $(\alpha\cdot a)$ runs through all elements of

$\mathfrak{M}$, and in which the sum of any two elements $A(\theta, (\alpha \cdot a))$, $A(\theta, (\beta \cdot b))$ is $A(\theta, (1, s))$, and their product is $A(\theta, (1, p))$. Evidently

$$\frac{\partial}{\partial \theta} A_n(\theta, (\alpha \cdot a)) = n A_{n-1}(\theta, (\alpha \cdot a)).$$

The further development belongs to the detailed applications of the subject, with which we are not concerned here. From the foregoing examples it is clear that any set of functions in a given variety generate, through the umbrae of their coefficients, irregular fields from which further irregular fields can be constructed by setting up correspondences with given functions. In the second example above the correspondence is with one of the simplest functions in $\mathfrak{A}$, namely $(\theta + \gamma)^n$, where θ, γ are in $\mathfrak{A}$.

CHAPTER V

ARITHMETICAL STRUCTURE

NATURE OF GENERAL ARITHMETIC, §§ 1–2

1. Abstraction, doctrinal function, transformation by formal equivalence. In the preceding chapters we have seen fragments of arithmetical structure emerging from theories not primarily concerned with arithmetic although applicable to it. The question thus arises as to what extent any theory is arithmetic. In any instance the answer must at present be more or less indefinite if, as suggested in Chapter I, there exists no agreement concerning what can legitimately be called arithmetic. One kind of generalization would draw no sharp distinction between algebra, arithmetic and analysis. From the point of view adopted here this is a misconception; the whole subject becomes entirely too simple and too structureless to be of interest unless it preserves the central features of rational arithmetic $\mathfrak{R}$, namely the existence of integral elements and their unique factorization.

What follows is merely a series of proposals toward an arithmetical theory of the structure of any theory constructed in accordance with the accepted processes of logic; it is an attempt to suggest a reason for the constant recurrence in theories applicable to the theory of numbers of an abstract structure which is itself arithmetical. It is complete in no detail. Whatever interest it may have lies in its attempt to show the need for more extensive postulational formulations of the several divisions of rational arithmetic than have been attempted, and in its indication of a new type of arithmetization which perhaps goes deeper than any yet proposed. With the injection of Dickson arithmetics into the theory of numbers it is apparent that "general arithmetic" in the classic sense of Dedekind and Kronecker is too restricted. This indicates

one direction in which generalizations of the theory of numbers may be sought. Another, to be sketched here, is less of a generalization than an abstraction. Its applications will be chiefly to the comparison of existing generalizations and to the exhibition of such abstract identities of form as are concealed beneath their various interpretations. The detailed application of the suggested program to even the simpler theories of arithmetic is a difficult matter, and is beyond the scope of the present chapter, although considerable progress has been made by my students. The project is feasible, but needs patience for its complete elaboration.

The point of view will be obvious to anyone acquainted with the General Analysis of E. H. Moore, as developed in his Colloquium Lectures, 1910, and in his lectures at the University of Chicago, or with the concept of *doctrinal functions* as stated by C. J. Keyser (*Concerning multiple interpretations of postulate systems, etc., Journal of Psychology and Scientific Method,* New York, vol. 9 no. 10, 1913) or again with the abstractly identical concept of the *system functions* of H. M. Sheffer (*The General Theory of Notational Relativity,* mimeographed, Cambridge, Mass. 1921). For an accessible account of the doctrinal function (we shall use Keyser's convenient term) we refer to his *Introduction to Mathematical Philosophy*, 1922, Lecture III. It will suffice here to recall that a doctrinal function is the extension to a system of postulates and their logical consequences, of the Whitehead-Russell propositional function. The doctrinal function of a given part of rational arithmetic, say the theory of divisibility, is what we shall call the *general theory* of that part. Interpretations (obtained by assigning to the marks in the doctrinal function specific meanings such that the truth value of the function is + (= true)) are, as before, called *instances* of the general theory. Since the introduction of doctrinal functions into mathematics it is improper to call any instance a general theory. This applies in particular to what is sometimes called "general arithmetic". For each of the several parts of rational arithmetic, such as the theory of the G.C.D.,

L. C. M., congruences, etc., there is precisely one doctrinal function; the set of all such, from the present point of view, is *arithmetic*—we may drop the qualification general. A value of the doctrinal function is an instance of arithmetic, but it is not itself arithmetic. Two complete instances of arithmetic have yet to be constructed; of the many partial instances the majority refer to the multiplicative side of arithmetic. It can be decided to what extent any theory T is arithmetic by setting up its doctrinal function and comparing the result with arithmetic, and similarly for any generalization of arithmetic. Before proceeding to the sketch we shall recall some of the terms used, although this is not necessary if familiarity with the cited works be presupposed.

In each of the postulates of a given set T the letters signifying relations are replaced by *marks* (Boole, E. H. Moore) denoting variable relations, and similarly for the relata, the marks for the latter signifying variable elements. It is an advantage to choose for the marks symbols bearing no resemblance to the originals. Thus $a > b$ may be replaced by $R(*, \dagger)$ or $R(X, Y)$, etc. The logical constants in T are left unchanged. The result is the doctrinal function $C(T)$ of T. By assigning to the marks in $C(T)$ the interpretations which they have in T we recover T. It may be possible to assign another set of interpretations such that the result, $C(T_1)$, is a set of true propositions. Each such $C(T_1)$ is a value of $C(T)$. The problem for a given T is twofold; first, from T we are to construct $C(T)$, second, from $C(T)$ we are either to find its values given the elements (relata), or we are to show that it is impossible to assign such interpretations to the relations in $C(T)$ that, for the given elements, the truth-value of $C(T)$ is $+$. The first part of the problem can always be solved readily. To solve the second, the doctrinal functions for the given elements must be constructed. If none of these is $C(T)$ the problem has no solution. The last is in nature of an existence theorem; it is as impracticable as many of the standard processes of the theory of ideals.

Let $C(T)$, $C(\Theta)$ be distinct doctrinal functions. Then we shall call T a generalization of Θ only when the first of the following is true and the second false,

$$C(T) \supset C(\Theta), \qquad C(\Theta) \supset C(T);$$

if both implications are true, so that $C(T) :\equiv: C(\Theta)$, then T, Θ are *identical*. Instances $T_j\,(j = 1, 2, \cdots)$ of $C(T)$ are called *abstractly identical*.

If P, Q are propositions such that $P :\equiv: Q$, that is, $(P \supset Q) \cdot (Q \supset P)$, either of P, Q may replace the other in an implication involving either. The substitution is called *transformation by formal equivalence*. Its use is to transform given propositions into others more easily recognizable as being abstractly identical with other given propositions. For example, $a \equiv b \mod m$ in rational arithmetic may be replaced by the assertion that $a - b$ is in the class of integral multiples of m, in which form it is abstractly identical with congruence with respect to an ideal modulus.

2. **Moore's heuristic principle.** We have thus far two problems, (A) Given T, find $C(T)$; (B), given $C(T)$, find T. There is now the third problem (C), given $C(T)$, make $C(T)$ categorical and separate $C(T)$ into all possible parts $C_j(T)$ $(j = 1, 2, \cdots)$ such that each is categorical. Each $C_j(T)$ is a subtheory of $C(T)$. We have called $C(\mathfrak{N})$ where $\mathfrak{N}$ is rational arithmetic, arithmetic. From any T we are to isolate all $C_j(T)$ such that $C(\mathfrak{N}) . \supset . C(T)$. Let $j = a, b, \cdots, c, \cdots$ be these. Then the *arithmetic* of $C(T)$ is given by $j = a, b, \cdots, c, \cdots$. Suppose now that we are given $C(T)$. Then $C(T)$ may be minimized in the categorical sense, that is, from $C(T)$ are to be rejected all those of its elements which are implied by other of its elements. There remains an irreducible residue $C'(T)$ which implies $C(T)$. If the solution of problem (C) is apparently multiform, giving $C^{(j)}(T)$ $(j = 1, 2, \cdots)$, then $C^{(j)}(T) :\equiv: C^{(k)}(T)$, and the solutions are identical.

As already remarked, the actual solution of problem (B) is impracticable according to the method suggested by its

existence proof—a by no means rare characteristic of existence proofs in mathematics. In the practical attack on (B) a guide is the *heuristic principle* of Moore. This principle, now being accessible in the place cited, may be taken for granted; beautiful illustrations of it occur in the earlier papers of Dedekind on algebraic numbers and ideals, but it was first clearly formulated as a principle by Moore. In what follows this principle will be recognized as resident in the G. C. D. of two theories T, Θ. The extent to which two theories are unified with respect to their central features may be measured by their G. C. D.

The algebra of classes (and hence also of relations) is essentially arithmetical in structure. By structure we mean the form of a doctrinal function, leaving form undefined, (no satisfactory definition has yet been given) although it may be readily apprehended. For example, $a \supset b$ has the same form as $p \supset q$, while $a :\equiv: b$ and $p \supset q$ have different forms. It might be presumed that it would be a simple exercise to specify form by the logical constants and variables involved in a given $C(T)$. This however is not the case; it is in general easy to destroy any such attempted formulation by pointing out tacit assumptions as to order (one such occurs, for example, in classic postulates for order itself: "aRb and bRa are distinct"). We shall therefore assume the meaning of structure as known. That rational arithmetic and the algebra of classes should have much in common structurally is not unexpected since both are based on the discrete. It would be interesting to know which, if either, is logically precedent; it is more interesting to take as a hypothesis the assumption that logic and arithmetic are abstractly identical.

The link between arithmetic and structure appears in the fundamental dichotomy of logic. It will be necessary therefore to indicate how the algebra $\mathfrak{L}$ of classes (or of relations) may be exhibited as an instance of certain parts of arithmetic. Equivalents will be found in terms of classes and relations between them for the G. C. D., L. C. M., the theory of divisibility, the theory of congruences and unique factori-

zation into primes in the sense of rational arithmetic $\mathfrak{N}$. There is also a theory of forms for classes but, owing to the law of tautology, it is so rudimentary as to be negligible. The quotient in $\mathfrak{L}$ is not unique, that is, the algebra from which the arithmetic is constructed is not a division algebra, although (rather remarkably) the fundamental theorem of arithmetic holds. At least two methods of isolating those parts of the algebra of classes which are abstractly identical with parts of arithmetic are available. We may first seek a theory of divisibility and then construct a theory of congruences consistent with it, or we may take these steps in the reverse order. A chief objection to the first is the absence of a set of postulates broad enough to include all known instances of integral elements. By the second method, provided we can construct a theory of congruences, we are ipso facto given at least one possible choice of integral elements. We are not however thereby given a theory of residuation in the form of the division transformation which is the foundation of Euclid's algorithm for the G. C. D. The absence of the division transformation in a given theory however does not necessarily show that the theory is non-arithmetical in all respects; for example there may be a multiplicative theory, as is indeed the case for Dedekind ideals, where the transformation is lacking. According to the specific interpretations of the elements concerned one of the methods will usually have decided advantages over the other. When the elements are classes the methods are on a level, owing to the extreme simplicity of the algebra underlying the arithmetic. Hence in the present instance we may choose either; on account of its greater novelty of approach we shall first seek a theory (there is more than one) of congruence for classes.

ARITHMETIC $\mathfrak{L}_N$ OF $\mathfrak{L}$, §§ 3–7

3. Arithmetical congruence. For clearness we state the postulates for a ring $\mathfrak{R}$ that will be used. Consider a set Σ of elements $x, y, z, \cdots, u', z'$ and two operations S, P (= addition, multiplication) that may be performed upon

any two equal or distinct elements x, y of Σ, in this order, to produce uniquely determined elements $S(x, y)$, $P(x, y)$, such that the postulates (3.1)–(3.3) are satisfied. Elements of Σ will be called elements of $\mathfrak{R}$.

(3.1) If x, y are elements of $\mathfrak{R}$, then $S(x, y)$, $P(x, y)$ are uniquely determined elements of $\mathfrak{R}$, and

$$S(x, y) = S(y, x), \qquad P(x, y) = P(y, x).$$

(3.2) If x, y, z are any three elements of $\mathfrak{R}$, then

$$\begin{aligned} S(S(x, y), z) &= S(x, S(y, z)), \\ P(P(x, y), z) &= P(x, P(y, z)), \\ P(x, S(y, z)) &= S(P(x, y), P(x, z)). \end{aligned}$$

(3.3) There exist in $\mathfrak{R}$ two distinct unique elements, denoted by u', z', called respectively the *unity, zero* of $\mathfrak{R}$, such that, if x is any element of $\mathfrak{R}$, then

$$S(x, z') = x, \qquad P(x, u') = x.$$

Next, consider a *uniform relation* $C(x, y)$ in $\mathfrak{R}$, that is, $C(x, y)$ is uniquely significant for each pair (x, y) of elements x, y in $\mathfrak{R}$, such that the postulates (3.4) (3.7) are satisfied, where x, y, z, w are any elements of $\mathfrak{R}$.

(3.4) $$C(x, y) \mathrel{.\supset.} C(y, x),$$

(3.5) $$C(x, y) \cdot C(y, z) \mathrel{:\supset:} C(x, z),$$

(3.6) $$C(x, y) \cdot C(z, w) \mathrel{:\supset:} C(S(x, z), S(y, w)),$$

(3.7) $$C(x, y) \cdot C(z, w) \mathrel{:\supset:} C(P(x, z), P(y, w)).$$

The dot between relations or propositions signifies as usual the logical "and". We shall call C *algebraic congruence* in $\mathfrak{R}$.

Let $\mathfrak{N}$ denote rational arithmetic. If a, b, m are integers, an instance in $\mathfrak{N}$ of C is $C(a, b) \equiv (a \equiv b \bmod m)$, but C is not sufficient to define in $\mathfrak{N}$ the usual meaning of congruence. In addition we require

(3.8) $\qquad (a \equiv 0 \mod m) \mathrel{:\equiv:} m \mid a,\ m \neq 0,$

(3.9) $\quad (ka \equiv kb \mod m) \supset (a \equiv b \mod m'),\ m \neq 0,$

where $m \mid a$ is read in $\mathfrak{N}$ "m divides a", and where $qm' = m$ and $q =$ the G. C. D. of k, m. In these the sign $\equiv$ of arithmetic congruence will not be confused with $=$ meaning definitional identity and $:=:$ meaning formal equivalence. In $\mathfrak{N}$, (3.8), (3.9) may be replaced by any transforms of themselves by formal equivalence. We shall not distinguish such transforms in the determination of a doctrinal function. Any set of propositions (or postulates) abstractly identical with (3.8), (3.9) and an instance in $\mathfrak{N}$ of (3.4)–(3.7) will be called *arithmetic congruence* for the elements concerned.

The elements of L (the algebra of logic) will be denoted by Greek letters; thus $\alpha, \beta, \gamma, \cdots$ denote classes The null class ($=$ the zero of $\mathfrak{L}$) is ω, and the universal class ($=$ the unity of $\mathfrak{L}$) is ε; the (logical) sum, product of any two elements α, β of $\mathfrak{L}$ are written as usual $\alpha + \beta$, $\alpha\beta$ respectively. The supplement of any element of $\mathfrak{L}$ is indicated by an accent; thus α' is the supplement of α, and α' is the unique solution of $\alpha + \alpha' = \varepsilon$, $\alpha\alpha' = \omega$. It is assumed that if α, β are any elements of $\mathfrak{L}$, then so also are α', $\alpha\beta$, $\alpha + \beta$.

We proceed now to solve (3.4)–(3.7) in $\mathfrak{L}$. That is, we shall find in $\mathfrak{L}$ an instance of the doctrinal function defined by (3.4)–(3.7). By evident analogies with the theory of division for Dedekind ideals or for Kronecker modular systems we are led (among other possibilities) to the following. By $\alpha \mid \beta$ in $\mathfrak{L}$ we shall mean that α *contains* β, that is, each element of β is in α. Then an instance of (3.4)–(3.7) is given by either of

(3.10) $\qquad C(\alpha, \beta) \equiv \alpha\beta \mid \mu,$

(3.11) $\qquad C(\alpha, \beta) \equiv \mu \mid (\alpha + \beta),$

in which μ is an arbitrary constant element of $\mathfrak{L}$. Accordingly, in analogy with $\mathfrak{N}$ we may write (provisionally only,

since the equivalents in $\mathfrak{L}$ of (3.8), (3.9) in $\mathfrak{R}$ are yet to be satisfied),

$$(3.12) \qquad (\alpha \equiv \beta \bmod \mu) :\equiv: \alpha\beta \mid \mu,$$

$$(3.13) \qquad (\alpha \equiv \beta \bmod \mu) :\equiv: \mu \mid (\alpha + \beta).$$

That two solutions of (3.4)–(3.7) must exist in $\mathfrak{L}$, if one does, is evident from the dualism between addition and multiplication in $\mathfrak{L}$. This has no analogue in $\mathfrak{R}$.

Either of (3.12), (3.13) may be taken as the solution of the problem of algebraic congruence in $\mathfrak{L}$. To obtain arithmetic congruence in $\mathfrak{L}$ we must satisfy also any pair of equivalents of (3.8), (3.9), and for this we require the following considerations.

4. The arithmetic zero, unity in $\mathfrak{L}$; arithmetic division, addition and multiplication in $\mathfrak{L}$. We exclude division by zero in $\mathfrak{R}$ except in the one case when the dividend is zero, when, we shall say, the quotient exists and is indeterminate. This of course is not equivalent to saying that the quotient does not exist. If the quotient by zero is defined never to exist (which again is a radically different assertion from that which states that the quotient exists and is wholly indeterminate), we are forced into irreconcileable contradictions between $\mathfrak{R}$ and $\mathfrak{L}$, for $\omega\ \omega$ in $\mathfrak{L}$, while, according to the usual (loose) convention regarding division by zero in $\mathfrak{R}$, $0/0$ is without meaning. Our convention so far as $\mathfrak{R}$ alone is concerned alters nothing that is customary in $\mathfrak{R}$; with regard to $\mathfrak{L}$ it makes possible a complete isomorphism. This perhaps is a minor point, but for exactness it must be stated.

Consider in $\mathfrak{R}$ a relation D such that

$$(4.1) \qquad \therefore\ xDx,$$

$$(4.2) \qquad xDy \cdot yDz :\supset: xDz,$$

$$(4.3) \qquad xDy \cdot yDx :\supset: x = y,$$

where xDy is uniquely significant for each $x \neq z'$ ($z' \equiv$ the zero in $\mathfrak{R}$) and y in $\mathfrak{R}$, with the exception that $z'Dz'$ is

significant but indeterminate in $\mathfrak{R}$. An instance in $\mathfrak{N}$ of (4.1)–(4.3) is given by

$$x D y \equiv x \text{ divides } y.$$

This solution is valid also in $\mathfrak{A}$. If for $x \neq z'$ the truth value $+$ of $x D y$ implies the existence in $\mathfrak{R}$ of a unique w such that $y = P(x, w)$, the quotient in $\mathfrak{R}$ is said to be unique, and similarly in any instance of $\mathfrak{R}$. The solution in $\mathfrak{N}$ is unique; in $\mathfrak{A}$ it is not. This is in fact the distinction between a holoid and an orthoid realm. But, according to our provisional descriptions of arithmetic it is immaterial whether the quotient be unique provided only that the fundamental theorem of arithmetic subsists. In $\mathfrak{L}$ division as defined in a moment does not yield a unique quotient, but it does lead to unique factorization in the sense of $\mathfrak{N}$.

Analogy with the theory of ideals suggests that we take in $\mathfrak{L}$ either of the following,

$$\alpha D \beta \equiv \alpha \mid \beta, \tag{4.4}$$

$$\alpha D \beta \equiv \beta \mid \alpha. \tag{4.5}$$

Thus (4.4) states that in $\mathfrak{L}$ α *divides* β is identical with α *contains* β; (4.5) asserts that α *divides* β is identical with β *contains* α. As in determining $C(\alpha, \beta)$ a twofold solution (if one exists) is necessary by the dualism in $\mathfrak{L}$, and either implies the other. It does not yet follow that either of (4.4), (4.5) is an interpretation of division in $\mathfrak{L}$ which is consistent with algebraic congruence in $\mathfrak{L}$. To complete the solution we require the G. C. D., the L. C. M., and the zero, unity in $\mathfrak{L}$.

The G. C. D. and the L. C. M. are given by the following abstractions to $\mathfrak{R}$ of the G. C. D. and L. C. M. in $\mathfrak{N}$ after transformation by formal equivalence as suggested by the theory of ideals. (it is obvious that these functions can have no meaning in terms of order relations if they are to be significant for $\mathfrak{R}$, $\mathfrak{L}$ as well as $\mathfrak{N}$; hence the transformation).

Consider in $\mathfrak{R}$ two operations G, L upon elements of $\mathfrak{R}$ such that, x, y being in $\mathfrak{R}$, $G(x, y)$, $L(x, y)$ are uniquely determined elements of $\mathfrak{R}$ and the postulates (4.6)-(4.14) are satisfied.

(4.6) $\quad G(x, y), \quad L(x, y)$ are unique,

(4.7) $\quad G(x, y) = G(y, x),$

(4.8) $\quad G(x, G(y, z)) = G(G(x, y), z) \equiv G(x, y, z),$

the last of which defines $G(x, y, z)$;

(4.9) $\quad G(x, y) D x \cdot G(x, y) D y,$

(4.10) $\quad z D x \cdot z D y :\supset: z D G(x, y);$

(4.11) $\quad L(x, y) = L(y, x),$

(4.12) $\quad L(x, L(y, z)) = L(L(x, y), z) \equiv L(x, y, z),$

(4.13) $\quad x D L(x, y) \cdot y D L(x, y),$

(4.14) $\quad x D z \cdot y D z :\supset: L x, y) D z.$

For example, (4.13) asserts that in $\mathfrak{R}$, *x divides the L function of x, y and y divides the L function of x, y.* It would be more consistent to write $D(x, y)$ for $x \; D \; y$, but we have chosen the form used in order to recall its interpretation in $\mathfrak{R}$. Clearly the above are satisfied in $\mathfrak{R}$ by $G(a, b)$ = the G. C. D. of the integers a, b, and $L(a, b)$ = their L. C. M. In $\mathfrak{L}$ they are satisfied by either of the following, in which it is obviously necessary to take account of the twofold solution for D in $\mathfrak{L}$,

(4.15) $\quad \alpha D \beta \equiv \alpha | \beta, \quad G(\alpha, \beta) \equiv \alpha + \beta, \quad L(\alpha, \beta) \equiv \alpha \beta,$

(4.16) $\quad \alpha D \beta \equiv \beta | \alpha, \quad G(\alpha, \beta) \equiv \alpha \beta, \quad L(\alpha, \beta) \equiv \alpha + \beta,$

either of which follows from the other by the dualism in $\mathfrak{L}$.

It is now apparent that the addition $\alpha + \beta$ and the multiplication $\alpha \beta$ of $\mathfrak{L}$ are sufficient but not necessary for an *arithmetic $\mathfrak{L}_N$ of $\mathfrak{L}$*. In $\mathfrak{L}_N$ we shall define the zero ζ and the unity v by

(4.17) $\quad S(\alpha, \zeta) = \alpha, \quad P(\alpha, v) = \alpha,$

where S, P are as in either of the following,

$$(4.19) \qquad S(\alpha, \beta) = \alpha + \beta, \quad P(\alpha, \beta) = \alpha\beta,$$
$$(4.20) \qquad S(\alpha, \beta) = \alpha\beta, \quad P(\alpha, \beta) = \alpha + \beta,$$

and therefore $(\zeta, \upsilon) \quad (\omega, \varepsilon)$ in (4.19), while $(\zeta, \upsilon) = (\varepsilon, \omega)$ in (4.20). The unity in $\mathfrak{N}$ is the unique element which divides each element of $\mathfrak{N}$. In abstract identity with this we have in $\mathfrak{L}_N$,

$$(4.21) \qquad \alpha D \beta \equiv \alpha | \beta, \quad \upsilon = \varepsilon, \quad \upsilon D \gamma,$$
$$(4.22) \qquad \alpha D \beta \equiv \beta | \alpha, \quad \upsilon = \omega, \quad \upsilon D \gamma,$$

where γ is any element of $\mathfrak{L}$. Again, it is well known (*Principia Mathematica*, 1st edition, vol. I, p. 232, *24.13) that $\omega \; \omega$. In $\mathfrak{L}_N$ we have, abstractly identical with $\mathfrak{N}$,

$$\zeta | \gamma \cdot (\gamma \neq \zeta) \cdot (\zeta = \omega),$$
$$\gamma | \zeta \cdot (\gamma \neq \zeta) \cdot (\zeta = \varepsilon),$$

are false propositions,

5. **Recapitulation.** We define $\mathfrak{L}_N$ by either of the following columns (which are duals of one another in $\mathfrak{L}$).

Sum, $S(\alpha, \beta)$:	$\alpha + \beta$;	$\alpha\beta$;
Product, $P(\alpha, \beta)$:	$\alpha\beta$;	$\alpha + \beta$;
G. C. D., $G(\alpha, \beta)$:	$\alpha + \beta$;	$\alpha\beta$;
L. C. M., $L(\alpha, \beta)$:	$\alpha\beta$;	$\alpha + \beta$;
$\alpha \equiv \beta \bmod \mu$:	$\mu | (\alpha + \beta)$;	$\alpha\beta | \mu$;
zero, ζ:	ω;	ε;
unity, υ:	ε;	ω;
α *divides* β, $\alpha D \beta$:	$\alpha | \beta$;	$\beta | \alpha$,

in which α, β are any elements of $\mathfrak{L}$; ε, ω are the unity, zero in $\mathfrak{L}$, and $\alpha | \beta$ is read, "α contains, or includes, β". Either column gives an isomorph $\mathfrak{L}_N$ of $\mathfrak{N}$ in $\mathfrak{L}$ when, as presently, we complete congruence.

Order relations in $\mathfrak{N}$ are replaced in $\mathfrak{L}_N$ by the following. If in a given set of elements of $\mathfrak{L}_N$ there be a unique element different from the unity in $\mathfrak{L}_N$ which divides each element of the set, it is called the *lower extreme* of the set; if in

a given set there exists a unique element different from the zero in $\mathfrak{L}_N$ which is divisible by each element of the set, that element is called the *upper extreme* of the set. Division is of course to be taken in the sense of a definite one of the above duals, and the zero, unity in $\mathfrak{L}_N$ are taken from the same one. By the use of extremes "greatest" and "least" in the G. C. D. and L. C. M. can be restated in exact identity with $\mathfrak{R}$. For example, the "greatest" = the upper extreme, the "least" = the lower extreme, and the G. C. D. then becomes the "greatest" element of $\mathfrak{L}_N$ which divides each element of a given set; the L. C. M. becomes the "least" element of $\mathfrak{L}_N$ which is a multiple of each element in a given set. It is to be noticed that "greatest", "least" are not necessarily identical with "most inclusive", "least inclusive" respectively; the rôles with respect to inclusion may be the exact opposites of these. Further, the property in $\mathfrak{R}$ that the product of the G. C. D. and L. C. M. of two elements is equal to the product of the elements is preserved in $\mathfrak{L}_N$ (either type as above).

6. **Arithmetic congruence in $\mathfrak{L}_N$.** It is now clear that (3.8) in $\mathfrak{R}$ has in $\mathfrak{L}_N$ the equivalent

$$(\alpha \equiv \zeta \bmod \mu) :\equiv: \mu D \alpha. \tag{6.1}$$

To find the equivalent of (3.9) we need the concept of residuals as used in modular systems; the residual also exists in $\mathfrak{R}$. We shall first define it for $\mathfrak{R}$. If a, b, l, m are elements of $\mathfrak{R}$, in which the unity is u', such that m is uniquely determined by

$$[a D\{P(l, b)\}] \cdot [m D l] \cdot [m \neq u'], \tag{6.2}$$

(that is, if a divides the product in $\mathfrak{R}$ of l and b, and m also divides l, and m is different from the unity in $\mathfrak{R}$), where l runs through all elements of $\mathfrak{R}$, m is called the *residual bRa of b with respect to a*, and we write $m = bRa$. In $\mathfrak{R}$ the residual of k with respect to m is the quotient of m by the G. C. D. of k and m; hence it is m' in (3.9). In $\mathfrak{L}_N$, (6.2) becomes

(6.3) $[\alpha D\{P(\lambda, \beta)\}] \cdot [\mu D \lambda] \cdot [\mu \neq v] :\equiv: \mu \subseteq \beta R \alpha,$

where λ is an arbitrary element of $\mathfrak{L}_N$. Hence, in $\mathfrak{L}_N$, the abstractly identical equivalent of (3.9) in $\mathfrak{N}$ is

(6.4) $[P(\varkappa, \alpha) \equiv P(\varkappa, \beta) \bmod \mu] \supset [\alpha \equiv \beta \bmod \varkappa R \mu],$

which can readily be verified to be a true proposition for either form of $\mathfrak{L}_N$.

7. **The fundamental theorem of $\mathfrak{N}$ in $\mathfrak{L}_N$.** As remarked in Chapter I it is frequently profitable in seeking a unique factorization theorem to follow up any property of uniqueness for the elements considered. For example, from the unique expression of any symmetric function of given elements of $\mathfrak{N}$ in terms of the elementary symmetric functions of those elements we reach at once an isomorph of the multiplicative part of $\mathfrak{N}$ for symmetric functions, to which $\mathfrak{E}$ and its consequences can be immediately applied. For $\mathfrak{L}_N$ a sufficient property is given by Boole developments (*Laws of Thought*, Chapter V, especially Prop III; also Whitehead, *Universal Algebra*, Chapter II). All terms in a given development having zero coefficients are assumed to have been deleted. The product in $\mathfrak{L}$ of any two terms in a given development is the zero in $\mathfrak{L}$; the sum of all the terms is the unity in $\mathfrak{L}$. Hence if α, β are any distinct or identical (in which case $\alpha \subseteq \beta$) terms in a development, $\alpha \mid \beta \supset \alpha = \beta$. From a given set of classes $\mathfrak{L}$ is generated by the operations of logical addition, multiplication and taking of supplements; the Boole development of the (logical) unity of the set gives a set of terms such that the development of any element of $\mathfrak{L}$ as a sum in $\mathfrak{L}$ of such terms is unique. The dual development is also unique and is obtained by taking supplements of both sides of the original development of the supplement of the given element of $\mathfrak{L}$.

These considerations give us the fundamental theorem of $\mathfrak{N}$ in $\mathfrak{L}_N$. It is to be understood that addition, multiplication in $\mathfrak{L}_N$ refer to a definite one (either) of the columns in § 5. It is then easy to verify the following, where we

have arranged abstractly identical theorems and definitions from $\mathfrak{N}$, $\mathfrak{L}_N$ in parallel columns to show at a glance the isomorphism.

$\mathfrak{N}$	$\mathfrak{L}_N$
(7.11) If the G. C. D. of a, b is 1, then a, b are called coprime.	(7.12) If the G. C. D. of α, β is v, then α, β are called coprime.
(7.21) If k divides the product of a and b, and k, a are coprime, then k divides b.	(7.22) If $\varkappa$ divides the product of α and β, and $\varkappa$, α are coprime, then $\varkappa$ divides β.
(7.31) q is called prime if $k \neq 1$ divides q when and only when $k = q$.	(7.32) π is called prime if and only if $(\varkappa D \pi) \cdot (\varkappa \neq v) : \supset : \varkappa = \pi$.
(7.41) Primes exist; they may all be found by sifting (Eratosthenes), and they form a coprime set.	(7.42) Primes exist; they may all be found from the Boole development of ζ, and they form a coprime set.
(7.51) A positive integer is uniquely the product of primes.	(7.52) A given element of $\mathfrak{L}_N$ is the product of prime elements in one way only.
(7.61) The G. C. D. and L. C. M. of any set of positive integers can be written down from their resolutions as in (7.51).	(7.62) The G. C. D. and L. C. M. of any set of elements of $\mathfrak{L}_N$ can be written down from their resolution as in (7.52).
(7.71) By algebra $\mathfrak{E}$ the multiplicative properties of arithmetical functions are reduced to abstract identity with $\mathfrak{A}$.	(7.72) The same as (7.71), with obvious changes in notation.

The list can be indefinitely extended and we have already seen that the theory of congruences in $\mathfrak{N}$ goes over into $\mathfrak{L}_N$. In summary we can state that *the theory of class inclusion and that of congruences and divisibility in rational arithmetic are distinct values of one doctrinal function.*

The dual solution in § 5 abolishes any intrinsic distinction between "least" and "greatest" in the senses of „least in-

clusive", "most inclusive". Accordingly, when in the following we refer to G. C. D's and L. C. M's it is to be understood that our universe of discourse is a particular one of the columns in § 5, and that, throughout a given context, the same one of those columns is meant. The possibility that in a given theory sometimes one interpretation is used and sometimes the other, according to the end in view, may be ignored, as it leads to nothing essentially new, as can be easily shown.

ARITHMETIZATION, §§ 8–9

8. Classification of doctrinal functions. According to current definitions a doctrinal function is a set of postulates together with the set of all logical consequences of those postulates; a postulate is a propositional function, that is, the symbols of relations and elements (relata) are marks, and the relations and relata are variables. If specific interpretations can be assigned to the marks so that the resulting doctrinal function has the truth value $+$, we shall call the result (as before) a value or an instance of the function. In our present discussion we are interested in the functions themselves, not in their values. Let $C(T)$ be a doctrinal function. By the above (usual) definition $C(T)$ contains in general parts which are not logically independent of other parts. If from $C(T)$ we isolate $C_1(T)$ such that $C_1(T) \supset C(T)$ is true and $C_2(T) \supset C_1(T)$ is false if $C_2(T)$ and $C_1(T)$ are distinct, where $C_2(T)$ is a part of $C(T)$, we may call $C_1(T)$ a *reduced form* of $C(T)$, and we shall assume that if several reduced forms of $C(T)$ exist they are logically equivalent. This amounts to replacing $C(T)$ by its set of postulates. Henceforth we assume all $C(T)$'s to be reduced; a $C(T)$ is thus a class of propositional functions. Hence to the set of all $C(T)$'s we may apply $\mathfrak{L}_N$, resolving each $C(T)$ into its prime factors and thence determining the G. C. D and L. C. M of two or more. Thus $\mathfrak{L}_N$ gives us a means of classifying general theories with reference to their relations of inclusion with respect to implications, and this classification is abstractly

identical with the multiplicative properties of the positive rational integers. The algebra $\mathfrak{E}$ therefore is applicable to the study of abstract structure. It is not necessary, of course, in any of this, that the T from which $C(T)$ is constructed shall have any numerical significance. It is therefore perhaps not too much to say that the theory of logical structure is an instance of certain parts of $\mathfrak{N}$.

9. Nature of arithmetization. From a given theory Θ we construct its $C(\Theta)$, and we assume that we have already constructed $C(\mathfrak{N})$ ($\mathfrak{N}$ — rational arithmetic). Let the G. C. D in L of $C(\Theta)$, $C(N)$ be G. From G we have $C(G)$. Let the result of replacing in $C(G)$ all marks (of relations and relata) by their instances as in $C(\Theta)$, be $C(\Theta')$. Then if $C(\Theta')$ is a value of $C(G)$, we shall say that Θ is *arithmetized to the extent Θ' or that Θ' is the arithmetic of Θ.* This provides for the case where Θ has no arithmetic.

In the above we have taken $\mathfrak{N}$, rather than any of its current (partial) generalizations as the type of arithmetic. If it be desirable to replace $\mathfrak{N}$ be any of its partial generalizations, the procedure with respect to these is the same as with respect to $\mathfrak{N}$. It would be of interest first, however, to determine to what extent the existing extensions of $\mathfrak{N}$ are themselves arithmetic in the sense of $C(\mathfrak{N})$, for it seems that the ultimate difficulties of arithmetic reside in the natural numbers rather than in their extensions.

INDEX

(Numbers refer to pages)

Addition, 5.
algebra, common, 5.
arithmetic, 162–163.
— additive, 12.
— multiplicative, 12.
arithmetical theory, 11.
— complete, 11.
— improper, 11.
— proper, 11.
— restricted, 11.
arithmetization, 176.

Characteristic, 108.
— even, 108.
— odd, 108.
class numbers, 101–106.
composite, 113.
— E, 117.
congruence, 165.
— algebraic, 166.
— arithmetic, 167.
conjoint, 31.
— zero, 31.
conjugates, 32.
conjunction, 31.
coprime, 30.

Decomposition formulas, 48.
— in $\mathfrak{P}$, 50.
degree, algebraic, 63, 72.
— even, 40.
— odd, 40.
— of functional product, 110.
— of parity function, 40.
differentiation in $\mathfrak{C}$, 29.

Elements, 6, 8.
— equivalent, 9, 10.
elements, indecomposable, 9.
— integral, 124.
— irregular, 6, 18.
— regular, 6, 18.
— special, 18.

Field, 5.
— abstract, 5.
— irregular, 5.
— C-matric, 19.
— D-matric, 19.
— umbral, 155.
form, 80.
— even, 81.
— odd, 81.
— of order k, 80.
function, 11, 16.
— arbitrary, 107.
— associated, X, C, D, 20.
— base of primary, 116.
— circular in $\mathfrak{A}$, 77.
— codivisor of, 57.
— composite, 123.
— comultiple of, 57.
— derived, 114.
— divisibility of, 56.
— equality of, 56.
— factorable, 127.
— G. C. D. of, 58.
— L. C. M. of, 58.
— multiple of, 56.
— numerical, 144.
— parity, 66.

function, primary, 113, 115.
— prime, 123.
— quasi-even, 108.
— quasi-odd, 108.
— rational, 123.
— reciprocal, 123.
— type of, 69.
— uniform, 16, 115.
— vanishing over matrix, 55.

General theory, 161.
generator, 121.
— equality of, 121.
— fundamental, 123.
— integral, 124.
— rational, 123.
— reducible, 123.

Identity, abstract, 5.
index, 158.
instance, 5.
integer, simple 127.
integration in $\mathfrak{C}$, 29.
invariants, 92.
isomorph, 44.

Manifoldness, 128.
matrix, 15.
— absolute product of, 16.
— algebraic, 122.
— C, 15.
— conjoint, 31.
— coprime, 30, 41.
— D, 15.
— equality of, 15, 16.
— in $\mathfrak{B}$, 15.
— normal, 15.
— order of, 15, 16.
— partition of, 33.
— scalar product of, 16.
— transcendental, 122.
— zero, 16.
module, 7.
multiplication, 5, 8.
— C, 19, 20.
multiplication D, 19.
— of parities, 42.
— multiplicity, 128.

Negative, 6, 19.

Order, compound, 83.
— even, 40.
— of matric variable, 17.
— odd, 40.
— of parity function, 40.

Paraphrase, principle, 67.
— extended form of, 79.
— extension to higher forms, 80-88.
— integration of, 87.
— modified principle, 68.
parameter, 20.
parity, 36.
— absolute, 37–39.
— even absolute, 36.
— multiplication of, 42.
— odd absolute, 36.
— product of, 42.
— relative, 37.
— relative coprime, 41.
— transform, 62.
parity function, 66.
— restricted, 66.
partition, 33.
primary, 113.
— form, 113.
product, 5, 6, 8.
— absolute, 16.
— C, 19, 20.
— D, 19.
— E, 118.
— matric, 31.
— partial, 19.
— of parities, 42.
— scalar, 16.
— of sets, 56.
— symbolic, of functions, 109.

Quasi-constant, 109.
quotient, 7.

Ray, 7.
reciprocal, 7, 8, 19.
relation, uniform, 166.
representation, 81.
— compound, 81.
— compound limited, 87.
— limited, 85, 86.
— limited compound, 87.
— as sums of squares, 103.
residue, positive, 32.
ring, 7.
— modified, 114.

Scalar, 16.
— instance, 149.
— product, 16.
semigroup, 8.
— arithmetical, 11.
— associated, 23.
— commutative, 8.
— improper, 11.
— proper, 11.
series, exponential, 29.
— power, 28.
sets, 15.
— codivisor of, 56.
— comultiple of, 56.
— division of, 56.
— equality of, 56.
— G. C. D. of, 57.
— L. C. M. of, 57.
— product of, 56.
— sum of, 56.
— total, 56.
simple, 127.
substitution groups, 92.
sum, 5, 6, 32.
— C, 19, 20.
— D, 19.
— E, 118.
— matric, 31.
sum, partial, 19.
— of sets, 56.

Theta, 64.
— quotient, 64.
— of p arguments, 106.
trace, 32.
transform, 62.
transformation, 62.
— identical, 49.
— parity, 62.

Umbra, 29, 147.
unit, 9, 10.
unitary, 83, 86.
unity, 5, 8, 18, 118.

Variable, 17.
— coprime matric, 30.
— integral value of matric, 80.
— matric, 17.
— scalar, 17.
— value of, 17.
variety, 5.
— functional, 21.
— taken over $\mathfrak{A}$, 26.
— $\mathfrak{A}$, $\mathfrak{A}_f$, 5.
— $\mathfrak{B}$, 14, 28.
— $\mathfrak{B}_\infty \mathfrak{A}$, 27.
— $\mathfrak{B}_\infty \mathfrak{U}_m$, 26.
— $\mathfrak{B}_{\infty,\varphi} \mathfrak{U}_m$, 26.
— $\mathfrak{C}$, 13, 27.
— $\mathfrak{C}_\infty \mathfrak{A}$, 27.
— $\mathfrak{C}_\infty \mathfrak{U}_m$, 19, 23.
— $\mathfrak{C}_n$, $\mathfrak{U}_m$, 19.
— $\mathfrak{D}$, 13, 28.
— $\mathfrak{D}_\infty \mathfrak{U}_m$, 24.
— $\mathfrak{D}_n \mathfrak{U}_m$, 19.
— $\mathfrak{E}$, 13, 112, 119.
— $\mathfrak{E}_r$, 125.
— $\mathfrak{F}$, $\mathfrak{F}_c$, $\mathfrak{F}_r$, 5.
— $\mathfrak{G}$, 8, 121.
— $\mathfrak{G}_C$, 23.
— $\mathfrak{G}_D$, 22, 23.
— $\mathfrak{G}_E$, 123.

variety $\mathfrak{G}_x$, 22.
— $\mathfrak{FF}$, 6.
— $\mathfrak{FU}$, 155.
— $\mathfrak{L}$, 164.
— $\mathfrak{L}_N$, 164, 170.
— $\mathfrak{M}$, 7.
— $\mathfrak{N}$, 160.
— $\mathfrak{P}$, 14, 34, 46.
— $\mathfrak{R}$, 7, 160.
— $\mathfrak{R}_\varphi$, 44.
— $\mathfrak{S}_C$, 24.
— $\mathfrak{S}_D$, 24.
— $\mathfrak{T}$, 44.
variety $\mathfrak{T}_u$, 150.
— $\mathfrak{U}$, 5.
— $\mathfrak{U}_m$, 5.
— $\mathfrak{U}_\infty$, 6.
— $\mathfrak{V}$, 5.
— $\mathfrak{X}_\infty \mathfrak{U}_m$, 23.
— $\mathfrak{X}_{\infty,\varphi} \mathfrak{U}_m$, 23.
— $\mathfrak{X}_n \mathfrak{U}_m$, 20.
— $\mathfrak{X}_{n,\varphi} \mathfrak{U}_m$, 21.
— $\mathfrak{Y}_\infty \mathfrak{A}$, 27.
— $\mathfrak{Y}_{\infty,\varphi} \mathfrak{A}$, 27.

Zero, 5, 18.